eSTRATEGY 55
02/23
Das Digital Enablement Magazin

Cybersecurity im Mittelstand

DIGITAL BUSINESS

Psychologie und UX-Design: Deshalb gehen sie Hand in Hand

MANAGEMENT

Wie B2B-Surveys das wirtschaftliche Wachstum von Unternehmen beflügeln

CYBERSECURITY

Cybersecurity im Mittelstand – Experteninterview

E-COMMERCE

Web Push und Tracking im E-Commerce

published by TechDivision

568160353 / Adobe Stock

Cybersecurity im Mittelstand

Die Digitalisierung hat Unternehmen auf der ganzen Welt in eine neue Ära des Geschäftslebens und der Kommunikation geführt. Gleichzeitig nehmen Cyberangriffe stetig zu und haben in den letzten Jahren alarmierende Ausmaße angenommen. Laut dem Cybersecurity Ventures Bericht werden die weltweiten Kosten für Cyberkriminalität bis 2025 voraussichtlich 10,5 Billionen US-Dollar erreichen. Dies verdeutlicht die Dringlichkeit, effektive Maßnahmen zur Stärkung der Cybersecurity zu ergreifen.

In unserem Leitartikel befassen wir uns für Sie mit den aktuellen **Entwicklungen, Daten und Fakten zum Thema Cybersecurity**. Wir erörtern die häufigsten Schwachstellen und Angriffsverfahren und geben wichtige Tipps, insbesondere für mittelständische Unternehmen, um die Cybersecurity zu verbessern. Zudem haben wir für Sie einige **Best Practices** für den Worst-Case **nach einem Angriff** zusammengestellt.

Machen Sie sich wieder auf spannenden Lesestoff rund um **E-Commerce** und **Digital Business** gefasst. Es erwarten Sie einige interessante Interviews – auch ein Experteninterview zur Thematik **Cybersecurity im Mittelstand**. Zudem erfahren Sie u. a., warum **Psychologie und UX-Design** Hand in Hand gehen, wie **B2B-Surveys** das wirtschaftliche Wachstum von Unternehmen beflügeln, wie Sie **Web Push und Tracking im E-Commerce** als Umsatz-Boost nutzen können, welche **Cybersecurity-Maßnahmen im B2B Commerce** angebracht sind und erhalten Tipps zur **Verkaufspsychologie in Videos**.

In diesem Sinne wünschen wir Ihnen eine aufschlussreiche Lektüre. Passen Sie auf sich auf und bleiben Sie gesund!

Ihr Josef Willkommer
Herausgeber & Chefredakteur

TechDivision

Und jetzt nochmal mit Gefühl!

Ganz egal, welche Software Sie einsetzen, wie gut Ihre Prozesse, wie perfekt Ihre Daten, wie hochwertig Ihre Medien, wie treffsicher Ihre Texte sind. Wenn Ihre Kund*innen nichts fühlen, ist alles umsonst.

Ja genau, fühlen. Erleichterung, das richtige Geschenk für einen geliebten Menschen gefunden zu haben, Freude über das perfekte Reiseziel, Jagdfieber wegen dem Einzelstück im Sommerschlussverkauf, Dankbarkeit für den perfekten Service. Das ist das wahre Ziel der digitalen Transformation: Technik so einsetzen, dass sie Menschen glücklich und Ihre Marke zu einer Love Brand macht.

B2C und B2B, wo und wie auch immer. Deswegen ist Customer Experience Design der Schlüssel zu dem guten Gefühl, das eine richtig gute Lösung auslöst.

Und deswegen starten wir mit Ihnen genau dort: Beim Gefühl Ihrer Kund*innen.

www.techdivision.com

News

02 Editorial

Leitartikel

06 Cybersecurity im Wandel der Zeit

Digital Business

18 Was ist Master Data Management und warum ist es wichtig?
24 Psychologie und UX-Design: Deshalb gehen sie Hand in Hand
29 Diese vier Vorteile bietet serverseitiges Tag-Management

Cybersecurity

33 Alles, was Sie über die NIS-2-Richtlinie der EU wissen sollten
38 Cybersecurity im Mittelstand – Experteninterview
44 Richtig auf Hackerangriffe reagieren
48 Cybersecurity-Maßnahmen im B2B Commerce
52 Mitarbeiter-Manipulation Social Engineering

Management

59 Trends im Recruiting

24

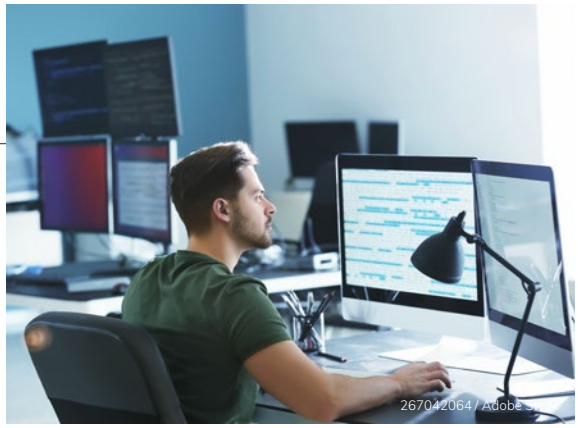
Psychologie und UX-Design: Deshalb gehen sie Hand in Hand

Der Erfolg eines digitalen Produkts hängt von der User Experience ab. User aber sind Menschen – sie können ungeduldig sein, Fehler machen, haben ein begrenztes Gedächtnis und eine begrenzte Aufmerksamkeitsspanne. Wie kann man also das UX-Design sinnvoll gestalten und die Aufmerksamkeit in die gewünschte Richtung lenken?

38

Cybersecurity im Mittelstand – Experteninterview

In unserer digitalisierten Wirtschaft ist das Risiko von Cyberangriffen allgegenwärtig. Insbesondere der Mittelstand gerät zunehmend ins Visier von Hackern. Doch welche spezifischen Schwachstellen und Herausforderungen betreffen mittelständische Unternehmen und was ist zu tun, wenn der Worst-Case eingetreten ist?



48

Cybersecurity-Maßnahmen im B2B Commerce

Drei Viertel der B2B-Unternehmen sehen einen Anstieg der Betrugsversuche und wollen sich infolgedessen stärker auf den Nachweis digitaler Identitäten konzentrieren. Der Wunsch auf Nutzerseite: Nachhaltige Lösungen für die Identitätsprüfung in Onlineshops.

Management

63 Wie B2B-Surveys das wirtschaftliche Wachstum von Unternehmen beflügeln

68 Feedback als Lösung gegen Personalabwanderung

E-Commerce

71 Web Push und Tracking im E-Commerce

76 Produktdatenmanagement, PXM & Co. – Interview mit Akeneo Co-Founder

Online-Marketing

81 Erfolgschancen im B2B-Marketing erkennen

86 Verkaufspsychologie in Videos

91 Impressum

63

Wie B2B-Surveys das wirtschaftliche Wachstum von Unternehmen beflügeln

Verzichten Unternehmer auf eine kontinuierliche Optimierung ihres Waren- und Serviceangebots, riskieren sie, dass wertvolle Bestandskundschaft unbemerkt zu Mitbewerber*innen abwandert. Können Kundenzufriedenheitsumfragen diesem Dilemma entgegenwirken?

71

Web Push und Tracking im E-Commerce

Der Corona-bedingte Boom im E-Commerce klingt ab. Die neue Normalität hat für mehr Konkurrenz im Onlinehandel gesorgt, während die Finanzierung im Onlinebusiness heute deutlich schwieriger geworden ist. Daher steht Profitabilität jetzt im Fokus. Kann Web Push den Traffic im Shop steigern und den Umsatz gezielt ankurbeln?

86

Verkaufspsychologie in Videos

Mit einem fundierten Verständnis der Werbepsychologie können conversionstarke Videos erstellt werden, die die Aufmerksamkeit Ihrer Zuschauer effektiver auf sich ziehen und deren Verhalten positiv beeinflussen. Aber wie geht das genau und welche verkaufspsychologischen Techniken eignen sich hierfür?

568160353 / Adobe Stock

Cybersecurity im Wandel der Zeit

von Josef Willkommer

Wie sich mittelständische Unternehmen schützen können

Die digitale Transformation hat Unternehmen auf der ganzen Welt in eine neue Ära der Kommunikation und des Geschäftslebens geführt. Gleichzeitig hat sie jedoch auch die Risiken und Bedrohungen durch Cyberangriffe dramatisch erhöht. Cyberkriminelle nutzen immer ausgefeiltere Techniken, um vertrauliche Informationen zu stehlen, Systeme zu infiltrieren und Unternehmen finanziell zu schädigen.

In diesem Artikel befassen wir uns mit aktuellen Entwicklungen, Daten und Fakten zum Thema Cybersecurity. Darüber hinaus werden wir die häufigsten Schwachstellen und Angriffsverfahren erörtern und wichtige Tipps insbesondere für mittelständische Unternehmen geben, um ihre Cybersecurity zu verbessern. Zudem versuchen wir einige Best Practices für den Worst-Case nach einem Angriff zu geben.

Was steckt hinter Cybersecurity?

Cybersecurity, auch bekannt als IT-Sicherheit oder Informationssicherheit, bezieht sich auf den Schutz von Computersystemen, Netzwerken, Daten und elektronischen Informationen vor unbefugtem Zugriff, Nutzung, Veränderung oder Diebstahl. Es beinhaltet Maßnahmen und Technologien, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten und die Systeme vor Schäden durch Cyberangriffe zu schützen.

Experten definieren Cybersecurity wie folgt:

Laut dem National Institute of Standards and Technology (NIST), einer US-Bundesbehörde, ist Cybersecurity „der Prozess des Schutzes von Informationen durch die Verhinderung, Erkennung und Reaktion auf Angriffe".

Gemäß der European Union Agency for Cybersecurity (ENISA) handelt es sich bei Cybersecurity um „die Fähigkeit einer Informationsgesellschaft, Netzwerke, Informationssysteme und darin enthaltene Informationen vor Cybergefahren zu schützen".

Zusätzlich dazu hat auch der Cybersecurity-Experte Bruce Schneier eine Definition gegeben: „Cybersecurity ist der Schutz von Informationen vor Diebstahl, Beschädigung oder Veränderung sowie vor unbefugter Nutzung oder unbefugtem Zugriff".

Diese Definitionen verdeutlichen, dass Cybersecurity ein umfassender Ansatz ist, der Technologien, Richtlinien, Verfahren und das Bewusstsein der Benutzer umfasst, um ein hohes Maß an Schutz vor den zunehmenden Bedrohungen der digitalen Welt zu gewährleisten. Es geht nicht nur darum, reaktive Maßnahmen zu ergreifen, sondern auch um proaktive Maßnahmen zur Risikominimierung und zur Gewährleistung einer kontinuierlichen Sicherheit.

Aktuelle Entwicklungen in der Cybersecurity

Cyberangriffe nehmen stetig zu und haben in den letzten Jahren alarmierende Ausmaße angenommen. Laut dem Cybersecurity Ventures Bericht werden die weltweiten Kosten für Cyberkriminalität bis 2025 voraussichtlich 10,5 Billionen US-Dollar erreichen. Dies verdeutlicht die Dringlichkeit, effektive Maßnahmen zur Stärkung der Cybersecurity zu ergreifen.

Nachfolgend auch noch einige weitere Daten und Fakten, die verdeutlichen wie wichtig und massiv das Thema inzwischen ist:

Vermutlich gab es in den letzten Jahren keinen größeren Trend im Bereich der Cybersicherheit als: „Angriffe auf die Lieferkette". Cybervorfälle wie die Sicherheitslücke beim Softwaremanagement-Anbieter SolarWinds und bei Log4j in der Open-Source-Welt gefährden Unternehmen in aller Welt. Das Analystenunternehmen Gartner prognostiziert, dass bis 2025 45 % der globalen Unternehmen in irgendeiner Weise von einem Angriff auf die Lieferkette betroffen sein werden.[1]

Die Zahl der gemeldeten Schwachstellen nimmt weiter zu. Der HackerOne 2022 „Hacker-Powered Security Report" ergab, dass ethische Hacker allein im Jahr 2022 mehr als 65.000 Schwachstellen entdecken konnten, was einem Anstieg von 21 % gegenüber 2021 entspricht.

Laut dem „The Global Risks Report 2022" des Weltwirtschaftsforums werden die von Unternehmen, Regierungen und Privatpersonen getroffenen Sicherheitsvorkehrungen durch die zunehmende Raffinesse der Cyberkriminellen zunehmend überflüssig.

Laut dem „2022 Official Cybercrime Report“ von Cybersecurity Ventures werden sich die Kosten der Cyberkriminalität im Jahr 2023 auf 8 Billionen Dollar belaufen und bis 2025 auf 10,5 Billionen Dollar ansteigen.

Während Unternehmen versuchen, ihre eigenen sensiblen Daten vor Angriffen zu schützen, werden Kundendaten in anfälligen Datenbanken auf der ganzen Welt gespeichert. Laut der „2022 Identity Fraud Study“ belaufen sich die Verluste durch Identitätsbetrug auf insgesamt 52 Milliarden US-Dollar und betreffen 42 Millionen Erwachsene alleine in den USA.

Gemäß dem Report „Cost of a Data Breach 2022“, einem von IBM und dem Ponemon Institute veröffentlichten Bericht, benötigen Sicherheitsteams durchschnittlich 277 Tage, um eine Datenschutzverletzung zu erkennen und einzudämmen.

Laut dem selben Bericht dauert es länger, Datenverstöße mit verlorenen oder gestohlenen Zugangsdaten zu identifizieren und sie kosten 150.000 US-Dollar mehr als der durchschnittliche Datenverstoß.

Häufige Schwachstellen und Angriffsverfahren

Es gibt eine Vielzahl von Cyberangriffen, die Unternehmen und Organisationen weltweit bedrohen. Nachfolgend die zehn häufigsten Arten von Cyberangriffen:

Phishing

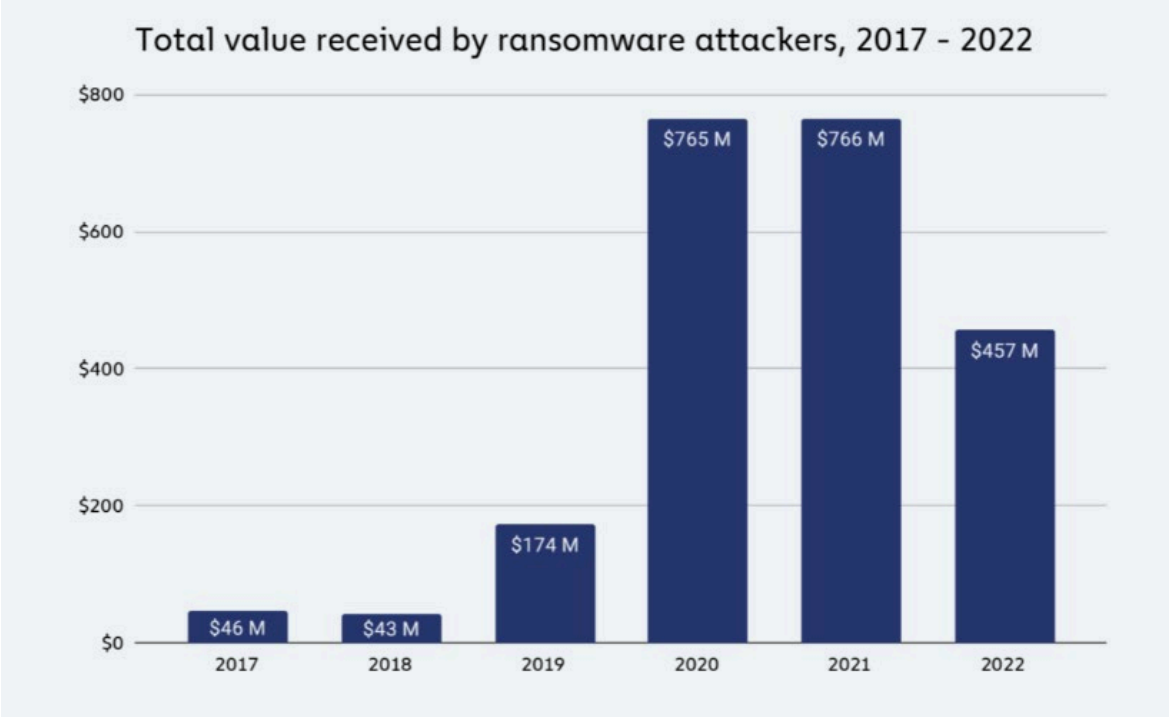
Ein absoluter Evergreen! Phishing ist eine betrügerische Methode, bei der Angreifer gefälschte E-Mails, SMS oder Websites verwenden, um an vertrauliche Informationen wie Passwörter, Benutzernamen oder Kreditkartendaten zu gelangen. Laut dem 2021 Data Breach Investigations Report von Verizon waren 36 % aller bestätigten Datenverletzungen im Jahr 2020 auf Phishing zurückzuführen. Phishing ist nach wie vor eine der häufigsten Bedrohungen für Unternehmen.

Das Anti-Phishing-System von Kaspersky verhinderte im Jahr 2022 mehr als 500 Millionen Versuche, auf betrügerische Websites zuzugreifen. Das ist doppelt so viel wie im Jahr 2021. Die am häufigsten verwendeten Köder für diese Angriffe waren Lieferdienste, Messenger und Kryptowährungsplattformen. Diese und weitere Ergebnisse finden Sie im neuen Kaspersky-Bericht über Spam und Phishing im Jahr 2022.

Nach Angaben des Unternehmens Lookout[2] wurde im Jahr 2022 die höchste Rate an mobilem Phishing in der Geschichte beobachtet, wobei jedes Quartal die Hälfte der Mobiltelefonbesitzer weltweit einem Phishing-Angriff ausgesetzt war. Der Lookout-Bericht basierte auf der Datenanalyse von Lookout von über 210 Millionen Geräten, 175 Millionen Apps und vier Millionen URLs täglich. In dem Bericht heißt es, dass „auch nicht-E-Mail-basierte Phishing-Angriffe zunehmen, wobei sich Vishing (Sprach-Phishing), Smishing (SMS-Phishing) und Quishing (QR-Code-Phishing) im zweiten Quartal 2022 versiebenfachen.“ Der Schaden kann für Unternehmen, die Opfer mobiler Phishing-Angriffe werden, gewaltige Folgen haben: Lookout hat errechnet, dass sich die potenziellen jährlichen finanziellen Auswirkungen von mobilem Phishing auf ein Unternehmen mit 5.000 Mitarbeitenden auf fast 4 Millionen US-Dollar belaufen.

Ransomware

Ransomware ist eine Form von Malware, die Computer oder Daten verschlüsselt und Lösegeld von den Opfern fordert, um die Daten wiederherzustellen. Laut dem Ransomware Report 2021 von Bitdefender stieg die Anzahl der Ransomware-Angriffe im Jahr 2020 um 715 %. Unternehmen waren besonders betroffen, wobei 69 % der Ransomware-Angriffe sich gegen Unternehmen richteten.



Bildquelle: https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

Nachfolgend einige alarmierende Statistiken über den Status von Ransomware- Angriffen:

- Im Jahr 2022 entdeckten Organisationen auf der ganzen Welt 493,33 Millionen Ransomware-Angriffe. Insgesamt stieg die Zahl der Ransomware-Angriffe zwischen dem dritten und vierten Quartal 2022 rapide an, nämlich von rund 102 Millionen auf fast 155 Millionen Fälle.
- Die durchschnittlichen Kosten eines Ransomware-Angriffs betrugen 1,85 Millionen Dollar.
- Statistiken zeigen, dass bis 2031 alle 2 Sekunden ein Ransomware-Angriff stattfinden wird.
- In der ersten Hälfte des Jahres 2022 gab es weltweit fast 236,7 Millionen Ransomware-Angriffe.
- Laut dem Verizon-Bericht über Datenschutzverletzungen 2022 haben Ransomware-Angriffe in den letzten fünf Jahren um 13 % zugenommen.
- Ransomware ist für 10 % aller Datenschutzverletzungen verantwortlich.
- 90 % der Ransomware-Angriffe hatten keinen Schaden zur Folge.
- Bei Ransomware-Verstößen dauerte es 49 Tage länger als im Durchschnitt, um sie zu identifizieren und einzudämmen.

Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS)

DoS- und DDoS-Angriffe zielen darauf ab, eine Website, einen Server oder ein Netzwerk durch Überlastung mit Anfragen außer Betrieb zu setzen. Laut dem State of the Internet / Security Report von Akamai stieg die Anzahl der DDoS-Angriffe im Jahr 2020 um 40 % im Vergleich zum Vorjahr. Besonders betroffen waren die Bereiche Gaming, E-Commerce und Gesundheitswesen.

Im Jahr 2022 entschärfte Microsoft durchschnittlich 1.435 Angriffe pro Tag. Die höchste Anzahl von Angriffen an einem Tag wurde am 22. September 2022 mit 2.215 Angriffen verzeichnet. Die geringste Anzahl von Angriffen an einem Tag lag bei 680 am 22. August 2022. Insgesamt hat Microsoft im Jahr 2022 nach eigenen Angaben mehr als 520.000 einzelne Angriffe auf deren globale Infrastruktur abgewehrt.[3]

Malware

Malware, eine Abkürzung für „malicious software“, umfasst verschiedene schädliche Programme wie Viren, Trojaner, Spyware und Würmer. Laut dem McAfee Threats Report im August 2021 stieg die Anzahl neuer Malware-Varianten im ersten Quartal 2021 um 43 %. Insbesondere Ransomware- und Krypto-Mining-Malware haben stark zugenommen.

Social Engineering

Social Engineering bezieht sich auf Manipulations- und Täuschungstechniken, bei denen Angreifer versuchen, Menschen dazu zu bringen, sensible Informationen preiszugeben oder bestimmte Aktionen auszuführen. Laut dem Verizon 2021 Data Breach Investigations Report sind 36 % der Datenverletzungen auf Social Engineering zurückzuführen, wobei Phishing-Angriffe eine häufige Methode sind.

Hierzu finden Sie in der aktuellen Ausgabe ein umfangreiches Interview mit Dr. Christian Schunck vom Fraunhofer IAO.

Insider-Angriffe

Insider-Angriffe erfolgen von Personen innerhalb des Unternehmens, sei es absichtlich oder versehentlich. Laut dem Insider Threat Report 2020 von Verizon sind 30 % der Datenverletzungen auf Insider-Angriffe zurückzuführen, wobei 23 % auf böswillige Insider und 7 % auf unbeabsichtigte Fehler oder Fahrlässigkeit von Mitarbeitenden entfallen.

SQL-Injections

Eine SQL-Injection ist eine Angriffstechnik, bei der Angreifer schädlichen SQL-Code in eine Datenbankabfrage einschleusen, um unerlaubten Zugriff auf Datenbanken zu erlangen oder diese zu manipulieren. Laut dem Web Application Attack Report 2020 von Akamai waren SQL-Injection-Angriffe für 65 % aller Webanwendungsangriffe im Jahr 2020 verantwortlich.

Obwohl diese Schwachstelle schon seit über 20 Jahren bekannt ist, rangieren Injections immer noch auf Platz 3 der OWASP Top 10 für Web-Schwachstellen. Im Jahr 2022 wurden 1162 Schwachstellen mit dem Typ „SQL-Injections“ als CVE akzeptiert. SQL-Injektionen sind daher nach wie vor ein Thema.

Dabei ist es immer wieder überraschend, wie häufig es selbst großen Organisationen nicht gelingt, SQL-Injections zu verhindern – obwohl der Markt voller kommerzieller und Open-Source-Tools ist, die behaupten, dies zu unterbinden. Nachfolgende Gründe begünstigen diese Methode nach wie vor:

- Den Entwicklern fehlt oft ein gewisses Sicherheitsbewusstsein.
- Es gibt kaum automatisierte und effiziente Testmethoden, die eine präzise Erkennung von Injektionen (z. B. ohne False Positives) ermöglichen.
- Bibliotheken für den Datenbankzugriff, die eigentlich einen sicheren Weg für den Zugriff auf DBs bieten sollten z. B. durch die Verwendung von Prepared Statements, können oft trotzdem missbraucht werden und geben dem Entwickler ein falsches Gefühl von Sicherheit.
- Fast jede Webanwendung verwendet irgendeine Form von Datenbank im Backend. Allein die Menge der SQL-Datenbanken bietet eine gewisse Angriffsfläche.

Open-Source-Schwachstellen

Open-Source-Software ist sehr weit verbreitet und häufig auch in proprietären Softwaretools enthalten, da sie einige Vorteile bietet. Wo Licht ist, ist aber häufig auch Schatten. So wurde laut Synopsys-Forschern in 84 % der Codebasen mindestens eine Open-Source-Schwachstelle gefunden. Die Schwachstellendaten wurden in den Open Source Security and Risk Analysis (OSSRA)-Bericht 2023 von Synopsys über Daten aus dem Jahr 2022 aufgenommen. Da die meisten Softwareanwendungen zumindest in Teilen Open-Source-Code enthalten, ist dies immer noch ein bedeutendes Cybersicherheitsproblem, das angegangen werden muss.

In dem Bericht heißt es: „In fast allem, was wir dieses Jahr untersucht haben, war Open Source enthalten. Es machte branchenübergreifend den Großteil der Codebasen aus“ und es wird ergänzt, „dass die Codebasen eine besorgniserregend hohe Anzahl bekannter Schwachstellen enthielten, die von Unternehmen nicht gepatcht werden konnten, wodurch sie anfällig für Exploits seien. Alle untersuchten Codebasen von Unternehmen aus den Bereichen Luft- und Raumfahrt, Luftfahrt, Automobil, Transport und Logistik enthielten teilweise Open-Source-Code, wobei Open-Source-Code 73 % des gesamten Codes ausmachte.“

So groß die Risiken durch den Open-Source-Code auch sind, sie können durch Penetrationstests und insbesondere durch Patching erkannt werden. Der Bericht stellte fest, dass Patches offensichtlich nicht angewendet wurden. Darin heißt es: „Von den 1.481 von den Forschern untersuchten Codebasen, die Risikobewertungen einschlossen, enthielten 91 % veraltete Versionen von Open-Source- Komponenten, was bedeutet, dass ein Update oder Patch verfügbar war, aber nicht angewendet wurde.“

Zero-Day-Exploits

Zero-Day-Exploits sind Schwachstellen in Software oder Betriebssystemen, die von Angreifern ausgenutzt werden, bevor sie von den Herstellern behoben werden können. Laut dem Zero Day Initiative Vulnerability Trends Report 2020 gab es im Jahr 2020 insgesamt 1.456 Zero-Day-Schwachstellen, von denen einige für Monate oder sogar Jahre ausgenutzt wurden, bevor sie entdeckt wurden.

Zu Jahresbeginn 2023 nutzte eine Ransomware-Bande eine neue Zero-Day- Schwachstelle, um Daten von einer Million Krankenhauspatienten zu stehlen. „Community Health Systems (CHS), einer der größten Gesundheitsdienstleister in den Vereinigten Staaten mit fast 80 Krankenhäusern in 16 Bundesstaaten, bestätigte, dass kriminelle Hacker auf die persönlichen und geschützten Gesundheitsdaten von bis zu 1 Million Patienten zugegriffen hatten. Der in Tennessee ansässige Gesundheitsriese gab in einer Einreichung bei den staatlichen Aufsichtsbehörden an, dass die Datenschutzverletzung auf die Verwendung einer beliebten Dateiübertragungssoftware namens GoAnywhere MFT zurückzuführen sei.“ [4]

Unter nachfolgendem Link finden Sie eine Liste aller öffentlich gemeldeten Sicherheitslücken, die von Forschern der Zero Day Initiative entdeckt wurden. Alle Sicherheitsschwachstellen, die von der Zero Day Initiative erfasst werden, werden gemäß der ZDI Disclosure Policy behandelt. Sobald der betroffene Hersteller die Schwachstelle behebt, wird ein begleitender Sicherheitshinweis veröffentlicht, der das Problem beschreibt und Links zu den Korrekturen des Herstellers enthält:
https://www.zerodayinitiative.com/advisories/published/

Advanced Persistent Threats (APTs)

APTs sind hochentwickelte und zielgerichtete Angriffe, die über einen längeren Zeitraum hinweg von Angreifern durchgeführt werden, um Zugang zu sensiblen Informationen zu erlangen. Laut dem 2020 Verizon Data Breach Investigations Report wurden 55 % der APT-Angriffe von organisierten kriminellen Gruppen durchgeführt, während 32 % staatlich unterstützte Angriffe waren. Weitere Infos zu APTs finden Sie im Advanced Persistent Threats Report 2022 von Seqrite.

Man-in-the-Middle (MitM) Angriffe

Ein Man-in-the-Middle (MitM)-Angriff ist eine Form des Cyberangriffs, bei dem ein Angreifer heimlich zwischen zwei Kommunikationsparteien tritt und die Kommunikation abfängt, abhört oder sogar manipuliert, ohne dass die beteiligten Parteien es merken. Der Angreifer positioniert sich buchstäblich „in der Mitte“ der Kommunikation und kann den gesamten Datenverkehr zwischen den Parteien überwachen und kontrollieren.

Ein erfolgreich durchgeführter MitM-Angriff kann schwerwiegende Konsequenzen haben. Der Angreifer kann vertrauliche Informationen stehlen, finanzielle Transaktionen manipulieren, E-Mails abfangen, Anmeldeinformationen erfassen und sogar Zugriff auf geschützte Systeme erlangen.

Es ist wichtig zu beachten, dass MitM-Angriffe verschiedene Formen annehmen können – je nachdem, welche Kommunikationsprotokolle oder Technologien verwendet werden. Dies können beispielsweise HTTPS-Verschlüsselung, E-Mail-Kommunikation, VoIP-Anrufe oder sogar mobile Apps sein. Daher ist es von entscheidender Bedeutung, starke Verschlüsselungstechnologien und andere Sicherheitsmechanismen zu verwenden, um das Risiko von MitM-Angriffen zu minimieren.

Laut dem Internet Security Threat Report von Symantec im Jahr 2021 stieg die Anzahl der MitM-Angriffe um 34 % im Vergleich zum Vorjahr.

Diese Daten und Fakten verdeutlichen die Bedrohlichkeit und die weitreichenden Auswirkungen der häufigsten Arten von Cyberangriffen. Unternehmen sollten daher umfassende Sicherheitsmaßnahmen ergreifen, um sich vor diesen Angriffen zu schützen und ihre Systeme, Daten und Netzwerke abzusichern.

TechDivision

BE STRONG. BE REAL. BE DIGITAL.

Du willst die digitale Zukunft mitgestalten?

Dann bist Du genau richtig bei uns!

Als erfolgreicher Webtechnologiedienstleister bietet Dir die TechDivision einen außergewöhnlichen Arbeitsalltag am Puls der Zeit.

MITARBEITENDE	STANDORTE	BÜROHUNDE	LEIDENSCHAFT
>160	6	9	100%

www.techdivision.com/karriere

karriere@techdivision.com

+49 8031 22 10 55-0

547147081 / Adobe Stock

10 Tipps zur Verbesserung der Cybersecurity für mittelständische Unternehmen

1. **Sensibilisierung der Mitarbeiter:** Schulen Sie Ihre Mitarbeiter regelmäßig über die Risiken von Cyberangriffen und wie sie diese erkennen und melden können.

2. **Starke Passwörter:** Fordern Sie die Verwendung von starken, eindeutigen Passwörtern für alle Konten und implementieren Sie eine Richtlinie zur regelmäßigen Passwortänderung.

3. **Zwei-Faktor-Authentifizierung (2FA):** Implementieren Sie die 2FA, um den Schutz der Konten zu verbessern und den Zugriff auf sensible Informationen zu erschweren. Beachten Sie jedoch, dass selbst 2FA keinen 100%-igen Schutz mehr bietet.

4. **Aktualisierte Software:** Stellen Sie sicher, dass Betriebssysteme, Anwendungen und Antivirenprogramme immer auf dem neuesten Stand sind.

5. **Sicherheitsrichtlinien:** Erstellen Sie klare Richtlinien für die Nutzung von IT-Ressourcen und stellen Sie sicher, dass sie von allen Mitarbeitenden befolgt werden.

6. **Datensicherung und Notfallwiederherstellung:** Führen Sie regelmäßige Backups Ihrer Daten durch und erstellen Sie einen Plan für den Ernstfall, um den Geschäftsbetrieb im Falle eines Cyberangriffs aufrechtzuerhalten.

7. **Netzwerksegmentierung:** Teilen Sie Ihr Netzwerk in separate Segmente auf, um den Zugriff auf sensible Daten zu beschränken.

8. **Echtzeitüberwachung:** Implementieren Sie eine Überwachungslösung, um verdächtige Aktivitäten in Echtzeit zu erkennen und darauf zu reagieren.

9. **Mitarbeiterzugriffskontrolle:** Gewähren Sie Mitarbeitenden nur die Berechtigungen, die für ihre Arbeit unbedingt erforderlich sind.

10. **Externe Unterstützung:** Ziehen Sie externe Experten hinzu, um eine umfassende Bewertung der Cybersicherheit durchzuführen, Penetrationtests durchführen zu lassen und Verbesserungsvorschläge zu erhalten.

Was tun, wenn der Worst-Case eingetreten ist?

Ein Cyberangriff kann jedes Unternehmen treffen, unabhängig von seiner Größe oder Branche. Die Folgen eines erfolgreichen Angriffs können schwerwiegend sein, angefangen von Datenverlust und Betriebsunterbrechungen bis hin zu Rufschädigung und finanziellen Verlusten. Im schlimmsten Fall kann sogar Insolvenz drohen. Angesichts der zunehmenden Anzahl und Raffinesse von Cyberangriffen ist es entscheidend, dass Unternehmen wissen, wie sie effektiv reagieren und sich erholen können. Nachfolgend finden Sie hierzu einige Tipps und Best Practices:

Sofortige Reaktion

Unmittelbar nach Feststellung des Angriffs ist schnelles Handeln erforderlich. „Es ist wichtig, den Vorfall umgehend zu melden und die betroffenen Systeme vom Netzwerk zu isolieren, um die Ausbreitung des Angriffs einzudämmen“, betont Dr. Jessica Barker, Cybersecurity-Expertin. Eine schnelle Reaktion minimiert potenzielle Schäden und ermöglicht es den Unternehmen, den Angriff besser zu untersuchen und die notwendigen Schritte zur Wiederherstellung zu planen. Aber vorsichtig: ein vorschnelles „Stecker ziehen“ kann gegebenenfalls wichtige Spuren und Informationen vernichten. Daher sollten Sie möglichst umgehend (externe) Cybersecurity-Experten hinzuziehen.

Informieren Sie die Behörden

„Ein Cyberangriff ist ein Verbrechen. Es ist wichtig, die zuständigen Behörden zu informieren“, sagt Brian Krebs, bekannter Sicherheitsexperte. Durch die Meldung des Vorfalls können Strafverfolgungsbehörden bei der Untersuchung helfen und mögliche Täter identifizieren. Unternehmen sollten auch in Erwägung ziehen, mit einem forensischen Experten zusammenzuarbeiten, um den Angriff gründlich zu analysieren. Hierzu stehen in Deutschland in jedem Bundesland zentrale Ansprechstellen Cybercrime der Polizei zur Verfügung. Weitere Infos und die entsprechenden Kontaktdaten finden Sie auf der Webseite der Polizei.

Kommunikation und Krisenmanagement

Transparente Kommunikation sowohl extern als auch intern ist entscheidend, um das Vertrauen der Kunden und Kundinnen sowie Geschäftspartner*innen aber auch der Mitarbeitenden aufrechtzuerhalten. „Informieren Sie umgehend Ihre Kunden und Stakeholder über den Vorfall und die Maßnahmen, die Sie ergreifen, um das Problem zu beheben“, rät Dr. Eric Cole, Cybersicherheitsexperte. Unternehmen sollten auch ein Krisenmanagement-Team einrichten, das die Kommunikation zentral koordiniert und den Wiederherstellungsprozess überwacht.

Wiederherstellung und Schwachstellenanalyse

Nach dem Angriff ist eine gründliche Wiederherstellung der Systeme und Daten erforderlich. „Stellen Sie sicher, dass alle Systeme vollständig bereinigt und gepatcht sind, um Schwachstellen zu schließen“, empfiehlt Theresa Payton, ehemalige CIO des Weißen Hauses. Eine gründliche Analyse des Angriffs hilft auch dabei, die Schwachstellen zu identifizieren und zu beheben, um zukünftige Angriffe zu verhindern. Hierzu sollten möglichst frühzeitig Cybersecurity-Experten involviert werden, um etwaige Spuren zu sichern und so Rückschlüsse auf entsprechende Angriffsvektoren und Schwachstellen ziehen zu können.

Verbessern Sie Ihre Sicherheitsmaßnahmen

Ein Cyberangriff sollte als Weckruf dienen, um die Cybersecurity-Maßnahmen zu verbessern. „Investieren Sie in fortgeschrittene Sicherheitstechnologien wie Intrusion Detection Systems, Endpunkt-Schutzlösungen und Sicherheitsschulungen für Mitarbeiter“, betont Bruce Schneier, renommierter Cybersecurity-Experte. Regelmäßige Sicherheitsaudits und Penetrationstests helfen dabei, potenzielle Schwachstellen zu identifizieren und zu beheben.

Überprüfen Sie Ihre IT-Richtlinien und Verfahren

Nach einem Angriff sollten Unternehmen ihre IT-Richtlinien und Verfahren überprüfen und aktualisieren. „Stellen Sie sicher, dass Ihre Richtlinien klare Anweisungen für den Umgang mit Sicherheitsvorfällen enthalten und dass Ihre Mitarbeiter über diese informiert sind“, sagt Graham Cluley, unabhängiger Sicherheitsexperte. Regelmäßige Schulungen und Tests unterstützen die Sensibilisierung der Mitarbeitenden für die Bedrohungen und helfen ihnen, sicherheitsbewusstes Verhalten zu entwickeln.

Überwachung und Incident Response

Implementieren Sie eine kontinuierliche Überwachung Ihrer Systeme, um potenzielle Angriffe frühzeitig zu erkennen. „Entwickeln Sie einen detaillierten Incident Response Plan, der klare Rollen und Verantwortlichkeiten für den Umgang mit Sicherheitsvorfällen festlegt“, rät Kevin Mitnick, ehemaliger Hacker. Ein effektiver Incident Response Plan ermöglicht eine schnelle Reaktion und begrenzt mögliche Schäden.

Zusammenarbeit mit externen Experten

In vielen Fällen ist es ratsam, mit externen Experten zusammenzuarbeiten, um den Wiederherstellungsprozess zu unterstützen und die Sicherheitsmaßnahmen zu verbessern. „Forensische Experten und Berater können wertvolle Einblicke liefern und bei der Implementierung robuster Sicherheitslösungen helfen“, sagt Mikko Hypponen, Chief Research Officer bei F-Secure.

Lernen Sie aus dem Vorfall

Ein Cyberangriff sollte als Lernerfahrung betrachtet werden. „Analysieren Sie den Vorfall gründlich, identifizieren Sie Schwachstellen und implementieren Sie Maßnahmen, um ähnliche Angriffe in Zukunft zu verhindern“, rät Dr. Eugene Spafford, renommierter Cybersecurity-Experte. Durch kontinuierliches Lernen und Anpassen können Unternehmen ihre Widerstandsfähigkeit gegen zukünftige Angriffe stärken.

Versicherungsschutz prüfen

Unternehmen sollten die Möglichkeit einer Cyberversicherung in Betracht ziehen. „Eine geeignete Versicherungspolice kann finanziellen Schutz bieten und den Wiederherstellungsprozess unterstützen“, betont Loretta Worters, Vizepräsidentin des Insurance Information Institute.

Fazit

Die Bedrohungen im Bereich der Cybersecurity sind real und können Unternehmen jeden Tag teuer zu stehen kommen. Mittelständische Unternehmen müssen proaktiv handeln, um ihre IT-Infrastruktur und sensible Daten vor Cyberangriffen zu schützen. Durch die Umsetzung effektiver Maßnahmen wie Mitarbeiter-Sensibilisierung, starke Passwörter, regelmäßige Updates und Notfallwiederherstellungspläne können Unternehmen ihre Cybersecurity erheblich verbessern und das Risiko von Angriffen minimieren. Es ist von entscheidender Bedeutung, dass Unternehmen ihre Sicherheitsmaßnahmen kontinuierlich überprüfen, aktualisieren und an neue Bedrohungen anpassen, um sich erfolgreich gegen Cyberkriminelle zu verteidigen.

Ein Cyberangriff kann verheerende Auswirkungen auf Unternehmen haben, aber eine angemessene Reaktion und Recovery-Strategie können helfen, die Schäden zu begrenzen. Durch die Umsetzung der genannten Schritte, unterstützt durch die Aussagen von Experten und Expertinnen, können Unternehmen nach einem Angriff ihre Sicherheitsmaßnahmen stärken, Schwachstellen identifizieren und sich besser gegen zukünftige Bedrohungen schützen. Die kontinuierliche Weiterentwicklung und Verbesserung der Cybersecurity ist ein wesentlicher Bestandteil der modernen Geschäftswelt, um den Schutz sensibler Daten und die Sicherheit und Zukunftsfähigkeit des Unternehmens zu gewährleisten.

AUTOR

Josef Willkommer

Chefredakteur eStrategy-Magazin

Als Mitgründer und Geschäftsführer der TechDivision GmbH, einer der führenden Adobe-Partner in der DACH-Region, beschäftigt sich Josef Willkommer seit vielen Jahren sehr intensiv mit E-Commerce, Digitalisierung und Online-Marketing. Darüber hinaus ist er als Chefredakteur des eStrategy-Magazins sowie als Autor diverser Fachbeiträge rund um E-Commerce und Digitalisierung auch journalistisch tätig. Neben diversen Beratungstätigkeiten für unterschiedlichste Unternehmen trifft man ihn bei diversen Fachkonferenzen zudem als Speaker zu E-Commerce- und Digitalisierungsthemen an.

www.techdivision.com
Josef Willkommer auf LinkedIn

Literatur & Links

[1] https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022
[2] https://www.lookout.com/form/the-global-state-of-mobile-phishing-report
[3] https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/
[4] https://techcrunch.com/2023/02/15/clop-ransomware-community-health-systems/

© Akeneo

Was ist Master Data Management (MDM) und warum ist es wichtig?

von Tobias Schlotter

In den meisten Unternehmen fließen Daten aus allen Quellen ein und werden von verschiedenen Abteilungen in unterschiedlichen Systemen gespeichert. Wenn dies der Fall ist, werden selbst die einfachsten Fragen zur Kundschaft oder Produkten schwierig zu beantworten sein. Glücklicherweise kann MDM in Kombination mit PIM helfen.

Daten sind für Unternehmen jeder Größe von entscheidender Bedeutung und die meisten Marken verfügen über eine große Menge davon. Aber die Macht der Daten liegt nicht darin, wie viele man sammelt, sondern darin, wie man sie verwaltet, analysiert und nutzt. Die richtige Nutzung von Daten kann zu einem enormen Wachstum führen … und, Sie ahnen es, eine falsche Verwaltung kann zu großen Problemen führen (denken Sie an doppelte Kundendatensätze, nicht übereinstimmende Produktinformationen und mehr).

Meist speichern verschiedene Abteilungen Daten aus allen Quellen in unterschiedlichen Systemen. Dadurch wird es selbst bei den einfachsten Fragen zu Kundschaft oder Produkten schwierig, sie genau zu beantworten.

Genau hier kann Master Data Management (MDM) helfen. MDM-Tools sind für Marken in allen Branchen von entscheidender Bedeutung, wenn es um die Bewältigung allgemeiner Probleme mit Produkt- und Kundendaten geht.

Was ist Master Data Management (MDM)?

Master Data Management schafft und verwaltet eine einzige, konsistente und genaue Quelle für Stammdaten in einem Unternehmen und kann daher auch als Stammdatenverwaltung bezeichnet werden. Es handelt sich dabei um eine Softwarekategorie, die verschiedene Datentypen zentralisiert und standardisiert, indem sie diese aus verschiedenen Systemen innerhalb eines Unternehmens verarbeitet, um einen „Master"-Datensatz zu erstellen. Diese Stammdaten sind die wesentlichen Daten, die in verschiedenen Systemen und Anwendungen – einschließlich PIM-Tools – gemeinsam genutzt und wiederverwendet werden.

Stammdaten können in vier Hauptdatenbereiche unterteilt werden:

- **Kunden:** Enthält Kundendaten wie Namen, Kontaktinformationen, Kaufhistorie und demografische Informationen. Wenn diese Daten genau und up-to-date sind, bedeutet dies eine effektivere Kommunikation, ein besseres Marketing und einen besseren Kundenservice.

- **Produkte:** Dazu gehören Daten wie Produktbeschreibungen, Merkmale, Preise und Lagerbestände. Daten aus dem Produktbereich helfen Unternehmen bei der Verwaltung ihrer Produktkataloge und bei der Rationalisierung der Lieferkettenabläufe.

- **Locations:** Enthält Daten wie Geschäftsadressen, Lagerstandorte und Versandrouten. Sie helfen Unternehmen, ihre Logistikabläufe zu optimieren und pünktliche und effiziente Lieferungen zu gewährleisten.

- **Sonstiges:** Machen Sie keinen Fehler: „Sonstiges" bedeutet nicht „unwichtig". Hier finden Sie Daten zu Lizenzen, Garantien, Verträgen, Mitarbeitenden und anderen wichtigen Geschäftsinformationen.

Was leistet eine MDM Software?

Stellen Sie sich MDM-Software wie einen großen, universellen Aktenschrank für alle Informationen Ihres Unternehmens vor – von Kundennamen und Adressen bis hin zu Produktbeschreibungen und Lagerbeständen.

MDM-Plattformen sind IT-gesteuerte Lösungen, die Harmonie in chaotische Technologiesysteme bringen. Einfach ausgedrückt bieten sie einen „goldenen Datensatz“ (auch bekannt als die „best version of the truth“) von wichtigen Geschäftsdaten, der das Potenzial für Redundanz, Duplizierung und Fehler eliminiert. Dies geschieht durch die Synchronisierung und Standardisierung von Daten im gesamten Ökosystem – was MDM zu einem wertvollen Tool für die Festlegung von Datenrichtlinien und -vorgaben, die Einhaltung gesetzlicher Vorschriften und die Verbesserung der Betriebseffizienz macht.

Der erstellte Stammdatensatz enthält die Kunden-, Produkt-, Standort- und Geschäftsdaten, die ein Unternehmen benötigt, um wichtige Aufgaben wie Marketingkampagnen, Serviceanrufe oder Verkaufsgespräche effektiver durchzuführen.

MDM-Software umfasst in der Regel Funktionen für Datenintegration, Datenqualität und Data Governance. Außerdem bietet sie Tools für die Verwaltung des Lebenszyklus von Stammdaten – von der Erstellung bis zur Stilllegung – um sicherzustellen, dass die Daten aktuell und relevant sind.

MDM vs. PIM

Ein Tool zur Zentralisierung von Daten und zur Erleichterung der Arbeit Ihrer Teams… klingt das bekannt? Das liegt daran, dass MDM und PIM (Product Information Management) beides Softwarelösungen sind, die Unternehmen bei der Verwaltung und Organisation ihrer Daten in eine einzigen „Informationsquelle“ unterstützen. Sowohl MDM als auch PIM erleichtern es allen Mitarbeitenden eines Unternehmens, wichtige Geschäftsentscheidungen auf der Grundlage genauer und konsistenter Informationen zu treffen.

Obwohl es Ähnlichkeiten zwischen den beiden Lösungen gibt, sollten Sie nicht davon ausgehen, dass sie austauschbar sind.

MDM spannt ein breiteres Datennetz und bietet eine einzige Informationsquelle für alle Arten von Daten. **PIM** hingegen ist technisch gesehen eine Teilmenge von MDM, die sich speziell auf die Verwaltung hochwertiger Produktinformationen konzentriert. PIM wird in der Regel von Marketing- und Vertriebsteams verwendet, um ihre Bemühungen bei der Vermarktung und Bewerbung von Produkten zu unterstützen.

Ich weiß, was Sie denken – wenn MDM alle Daten speichert und PIM nur Produktdaten, warum dann nicht auf PIM verzichten und die „All-in-One“-Lösung nutzen, die MDM-Plattformen zu bieten scheinen? Widerstehen Sie der Versuchung! MDM und PIM ergänzen sich gegenseitig, um ein unglaublich effizientes System für Marketing- und Vertriebsteams zu schaffen und letztlich ein verbessertes Produkterlebnis zu ermöglichen.

MDM-Plattformen können Produktdaten aus dem gesamten Ökosystem in einem einzigen PIM-System zusammenführen. Diese Informationen werden dann von Marketingfachleuten verbessert und mit den Assets im PIM kombiniert, bevor sie über alle Vertriebskanäle eines Unternehmens verteilt werden.

Was sind die Vorteile der Implementierung eines MDM?

Wir wissen, dass ein MDM eine universelle Datenquelle für Unternehmen schafft, aber warum ist das so wichtig? Die Implementierung eines MDM-Systems kann eine große Wirkung haben:

- **Erhöht die Datenkonsistenz:** Die „einzige Informationsquelle“, von der wir immer wieder sprechen, verringert das Risiko inkonsistenter oder ungenauer Daten, die dadurch entstehen, dass verschiedene Teams innerhalb des Unternehmens unterschiedliche Informationssysteme verwenden.

- **Bündelung von Kundeninformationen in einer einzigen Datenquelle:** MDM konsolidiert Kundendaten aus verschiedenen Quellen in einer einzigen Datensatzquelle, auf die autorisierte Benutzer*innen im gesamten Unternehmen zugreifen und sie aktualisieren können.

- **Verbessert die Produkt- und Kundenerfahrung:** Bessere Produkt- und Benutzerdaten bedeuten, dass Vertriebs- und Marketingteams effektiver arbeiten können. Außerdem führen diese Daten zu besseren Produktempfehlungen und einem individuelleren Kundenerlebnis.

- **Verbessert die interne betriebliche Effizienz:** Niemand verbringt gerne Zeit mit der Suche nach Daten aus anderen Abteilungen oder der manuellen Eingabe von Informationen in 10 verschiedene Systeme. Mit MDM-Tools lässt sich beides einsparen.

- **Hilft bei der Einhaltung von Datenvorschriften:** Um Kundendaten erfolgreich zu schützen, müssen Sie wissen, welche Art von Daten Sie besitzen, wo sie sich befinden und wie viele Sie besitzen. MDM kann Unternehmen dabei helfen, alle von ihnen erfassten personenbezogenen Daten zu identifizieren. Angesichts gesetzlicher Vorgaben wie dem Sarbanes-Oxley Act (SOX), dem Health Insurance Portability and Accountability Act (HIPAA), der GDPR der Europäischen Union und dem California Consumer Privacy Act (CCPA) ist MDM von großer Bedeutung.

Wie Sie das beste MDM für Ihr Unternehmen auswählen

Natürlich sind nicht alle MDM-Plattformen gleich. Die Wahl der richtigen MDM-Lösung für Ihr Unternehmen ist der Schlüssel zur Erhaltung hochwertiger Daten und zur Verbesserung der Effizienz. Auch wenn jedes Unternehmen seine eigenen Anforderungen hat, gibt es doch einige wichtige Merkmale, auf die Sie bei einer effektiven MDM-Lösung achten sollten.

Zum Beispiel sollten Sie sich für eine SaaS-basierte Plattform entscheiden, die in der Regel weniger Vorabinvestitionen in Hardware und IT-Infrastruktur erfordert und flexibler ist, wenn Ihr Unternehmen wächst.

Wachstum ist auch der Grund, warum Sie eine anpassbare MDM-Plattform benötigen. Wenn Sie wachsen, können sich Ihre Anforderungen an die Datenverwaltung ändern. Ihre MDM-Lösung sollte in der Lage sein, sich an diese Änderungen anzupassen. Stellen Sie sicher, dass die von Ihnen gewählte Lösung die Möglichkeit bietet, Workflows, Datenmodelle und vieles mehr nach Bedarf anzupassen.

Genauso wichtig wie „anpassbar“ ist „komponierbar“. Kompatible Software kommuniziert über eine API, was bedeutet, dass jede einzelne Lösung jederzeit aktualisiert oder ersetzt werden kann, ohne dass der Rest des Systems beeinträchtigt wird. Eine komponierbare MDM-Lösung ermöglicht auch eine einfachere Integration mit anderen Technologien in Ihrem Unternehmen, z. B. mit PIM-Systemen, Datenanalysetools oder anderen Geschäftsanwendungen. Auf diese Weise können Sie eine nahtlose Datenverwaltungsumgebung schaffen und Datensilos vermeiden.

Fazit

Unabhängig davon, ob Sie ein kleines Unternehmen sind, das gerade erst anfängt, oder ein großes Unternehmen, das sein Datenmanagement rationalisieren möchte, lohnt es sich, MDM-Software in Ihr Portfolio aufzunehmen. Sie kann nicht nur dazu beitragen, Datenverwaltungsprozesse zu rationalisieren, die Datengenauigkeit zu verbessern und die Konsistenz im gesamten Unternehmen zu erhöhen, sondern auch die Kunden- und Produkterfahrung erheblich zu verbessern. Mit dem richtigen MDM-System können Sie die Kontrolle über Ihr Datenmanagement übernehmen und sein volles Potenzial ausschöpfen.

AUTOR

Tobias Schlotter

Vice President Channel & Alliances EMEA bei Akeneo

Tobias Schlotter verantwortet als Vice President Global Channel das Partnerprogramm von Akeneo. Er studierte International Business & Management und sammelte mehr als zehn Jahre Erfahrung im Technologieumfeld, bevor er sich im Jahr 2015 Akeneo und dessen Vision von Product Experience Management (PXM) anschloss. Gemeinsam mit Partnern und einem stetig wachsenden lokalen Team widmete er sich zunächst dem Aufbau der Region Central & Eastern Europe, initiierte Kunden wie den Frankfurt Airport, Lamy, Liqui Moly, Brille24, Kneipp und Mytheresa und gewann so global agierende Marken, Händler und Marktplätze für das Akeneo PIM, bevor er seit Mitte 2022 das Partnergeschäft global mitverantwortet.

www.akeneo.com/de
Tobias Schlotter auf LinkedIn

akeneo

Product Cloud

Eine Lösung für Omnichannel-Commerce, die Besucher in Käufer verwandelt.

Akeneo Product Cloud ist die komplette und kompatible SaaS-Lösung, die Ihre Product-Story überall dort aktiviert, wo Ihre Kunden sind. Liefern Sie ansprechende, erstklassige Product Experiences über alle Ihre eigenen und fremden Kanäle mit Agilität und Präzision.

- Unschlagbare Time-to-Market
- Höhere Conversion Rates and Sales
- Geringere Retouren
- Höhere Kundenzufriedenheit und -treue
- Eliminierung redundanter Technologiekosten
- Flexibilität bei der Aktivierung des Produktdatensatzes für neue Kanäle

Demo anfordern

www.akeneo.com

578917773 / Adobe Stock

Psychologie und UX-Design

von Kateryna Kaida

Deshalb gehen sie Hand in Hand

Wenn wir die User Experience als Interaktion zwischen dem Menschen und der digitalen Welt betrachten, wird klar, dass menschliche Denkweisen das Design digitaler Produkte entscheidend beeinflussen können. Wir alle wissen, dass der Erfolg eines digitalen Produkts von der User Experience abhängt. Für ein gutes UX-Design braucht es also ein Verständnis der menschlichen Psychologie.

Gutes Softwaredesign ist nutzerzentriert und wie wir nicht vergessen dürfen, sind diese Nutzer*innen Menschen – Menschen, die ungeduldig und unmotiviert sein können, immer wieder Fehler machen und sowohl ein begrenztes Gedächtnis als auch eine begrenzte Aufmerksamkeitsspanne haben. Faktoren wie diese beeinflussen das alltägliche Verhalten der Nutzer*innen genau wie ihre Interaktionen mit digitalen Produkten wie mobilen Apps, Websites und Plattformen.

Wenn wir psychologische Prinzipien auf das UX-Design anwenden, können wir das gesamte Nutzungserlebnis sinnvoller und angenehmer gestalten. Wir können Produkte für eine Zielgruppe ansprechender gestalten, ihre Aufmerksamkeit lenken und sie dazu anregen, bestimmte Handlungen auszuführen.

Im Mittelpunkt: die Mensch-Computer-Interaktion

Der Bereich der Mensch-Computer-Interaktion (Human Computer Interaction bzw. HCI) untersucht, was an der Schnittstelle zwischen Nutzer*innen und digitalen Technologien geschieht. „Mensch" meint in diesem Kontext also eine Person, die mit dem System interagiert. „Computer" sind digitale Systeme oder Tools und „Interaktion" bezeichnet die Verbindung zwischen beiden.

Für jede Interaktion ist eine Schnittstelle erforderlich, etwa eine grafische Nutzeroberfläche (GUI) oder eine Sprachschnittstelle (VUI), die eine Kommunikation möglich macht. Diese Schnittstelle sollte intuitiv zu bedienen sein, sodass die Nutzer*innen alle gewünschten Handlungen durchführen können. Designteams, die ihren Fokus auf die Mensch-Computer-Interaktion legen, können bessere und effizientere Nutzeroberflächen (UIs) erstellen und das Nutzungserlebnis verbessern. Hierzu setzen sie meist eine Form des „Build-Measure-Learn"-Zyklus ein: Erst werden die Anforderungen und Wünsche der Nutzer*innen untersucht, dann eine UI erstellt und mit Nutzer*innen getestet. Anschließend werden die Ergebnisse analysiert und ins nächste Design übernommen.

Die Methoden und Studien aus dem Bereich Mensch-Computer-Interaktion können vor allem in drei Hauptbereichen angewendet werden: Technologien (z. B. Virtual Reality und mobile Schnittstellen oder Wearables), Fachgebiete (z. B. Sicherheit, Passwortsysteme wie CAPTCHA-Tests oder Spiele, bei denen Handlungen der Spielenden in Effekte und Ergebnisse übersetzt werden) und Ideen (z. B. verschiedene Methoden der Datenvisualisierung).

Die Bedeutung der kognitiven Psychologie

Sowohl HCI als auch UI und UX werden von der menschlichen Psychologie beeinflusst. Wenn wir eine für Menschen optimierte UI schaffen wollen, müssen wir bedenken, dass wir Menschen psychologisch komplex und gelegentlich irrational sind. Anders als bei Robotern oder automatisierten Systemen, deren Funktionsweisen streng nach logischen Prinzipien programmiert und konditioniert sind, hängen menschliche Handlungen und Entscheidungen von den unterschiedlichsten Faktoren ab – darunter Stimmungen, vorangegangene Erfahrungen, Voreingenommenheiten, die Umgebung und Stress.

Die kognitive Psychologie untersucht, wie Menschen denken und Informationen verarbeiten. Dabei betrachtet sie unsere internen mentalen Prozesse rund um Aufmerksamkeit, Gedächtnis und die Wahrnehmung der Welt um uns herum. Dazu kommen weitere Elemente wie Sprache, Problemlösung, Lernen und Metakognition bzw. Selbstreflexion. Drei Aspekte der kognitiven Psychologie haben einen besonders großen Einfluss auf HCI und UI/UX-Design:

- Unsere **Aufmerksamkeit** macht es uns möglich, uns auf bestimmte Dinge zu fokussieren. Hier geht es darum, wie erfolgreich wir spezifische Informationen erkennen und verarbeiten können und ob es uns gelingt, zu priorisieren und zu filtern, welche Informationen für eine Situation oder ein Ziel relevant sind und welche nicht.

- Unser **Gedächtnis** ist für das Speichern und Abrufen von Informationen verantwortlich und umfasst das Arbeitsgedächtnis sowie das Langzeitgedächtnis. Das Arbeitsgedächtnis speichert Informationen nur vorübergehend, während das Langzeitgedächtnis alle Informationen enthält, die in unserem gesamten Leben „gespeichert" werden. Das Arbeitsgedächtnis hat eine begrenzte Kapazität und kann durch Ablenkungen leicht beeinträchtigt werden.

- Die **Wahrnehmung** bezieht sich darauf, welche Informationen wir über unsere Sinne aufnehmen und wie wir sie interpretieren. Zu diesem Prozess gehört alles, was wir sehen, hören, berühren usw., ebenso wie die Art und Weise, wie wir die eingehenden Reize verstehen und wie sie unser Verhalten beeinflussen.

Wenn wir diese Prinzipien kennen und wissen, wie sie menschliche Reaktionen und Verhaltensweisen beeinflussen, haben wir bereits den Grundstein dafür gelegt, kognitive Psychologie auf das UI/UX-Design anzuwenden. Im nächsten Schritt nutzen wir dieses Wissen darüber, wie Aufmerksamkeit, Gedächtnis und Wahrnehmung funktionieren, um ein reibungsloseres und positiveres Nutzungserlebnis zu schaffen.

Psychologische Prinzipien im digitalen Produktdesign

Nobelpreisträger Daniel Kahneman geht davon aus, dass es zwei vollkommen unterschiedliche Prozesse gibt, die das menschliche Denken und die Entscheidungsfindung bestimmen: langsames Denken und schnelles Denken. Das langsame Denken ist für durchdachte Überlegungen und Analysen verantwortlich, während wir das schnelle Denken nutzen, wenn wir instinktive oder emotionale Entscheidungen treffen müssen. Beim Gestalten digitaler Erlebnisse sollten wir uns fragen, welcher dieser beiden Denkprozesse vermutlich gerade in unseren Nutzer*innen vorgeht, wenn sie mit unserem Produkt interagieren.

In den meisten Situationen verfolgt das UI-/UX-Design das Ziel, die Nutzeraktionen so mühelos und intuitiv wie möglich zu gestalten, damit die Nutzung keine Anstrengung erfordert. Allerdings sollten wir auch überlegen, an welchen Punkten der User Journey langsames Denken wichtig ist und unser Design entsprechend anpassen: An diesen Stellen können wir die Nutzer*innen ermutigend und motivierend dabei unterstützen, ihrem Ziel näherzukommen. Die folgenden psychologischen Prinzipien und Effekte können nützlich sein, um diese Ideen umzusetzen und eine bessere User Journey zu schaffen:

Zeigarnik-Effekt

Menschen neigen dazu, sich besser an die Einzelheiten nicht abgeschlossener Handlungen zu erinnern als an abgeschlossene Handlungen. Diesen Effekt können UI-Designteams sich zunutze machen, indem sie Fortschrittsbalken, Gamification-Elemente, Badges, Belohnungen und Ähnliches integrieren: So erhöhen sie die Aufmerksamkeit der Nutzer*innen, sodass sie sich besser auf die Aufgabe konzentrieren und sie erfolgreicher abschließen können.

Hicksches Gesetz

Je mehr Auswahlmöglichkeiten uns zur Verfügung stehen, desto schwieriger ist es, eine Entscheidung zu treffen. Für das Design von Nutzeroberflächen bedeutet das, die verfügbaren Optionen so weit wie möglich zu reduzieren. Wahlmöglichkeiten sollten mindestens in Kategorien aufgeteilt oder so präsentiert werden, dass sie leichter erfasst werden können – etwa indem empfohlene Optionen hervorgehoben werden, damit die Entscheidung einfacher wird.

Kognitive Überlastung

Wenn Nutzer*innen mit zu vielen Informationen oder gleichzeitig zu erledigenden Aufgaben konfrontiert werden, kann das zu kognitiver Überlastung führen. Daher sollten alle Arten von Ablenkungen reduziert werden, während Nutzer*innen Aufgaben ausführen. Bei komplexen Produkten oder Aufgaben sollten die Nutzer*innen als Erstes mit häufig genutzten Funktionen vertraut gemacht werden und die fortgeschrittenen Funktionen erst nach und nach kennenlernen.

Restorff-Effekt

Wenn Personen es mit mehreren ähnlichen Objekten oder Reizen zu tun haben, erinnern sie sich mit größter Wahrscheinlichkeit an diejenigen, die sich in ihrer Größe, Farbe oder einer anderen grundlegenden Eigenschaft von den anderen unterscheiden. Farben, 3D-Effekte, Bewegungen usw. können die Aufmerksamkeit von Personen auf ein bestimmtes Element (wie einen Call-to-Action oder eine Benachrichtigung) lenken. Damit das funktioniert, sollte nur dieses eine Element auf dem Bildschirm diese Eigenschaft aufweisen.

Fazit

Für ein gutes Produktdesign ist es unverzichtbar, sich mit Nutzerpsychologie und kognitiven Prozessen auszukennen. UI- und UX-Designer*innen, die damit vertraut sind, wie sich Aufmerksamkeit, Gedächtnis und Wahrnehmung auf das Verhalten und die Mensch-Computer-Interaktion auswirken, können ihre Nutzer*innen positiv beeinflussen und dafür sorgen, dass jedes Nutzungserlebnis zum Erfolg führt.

AUTORIN

Kateryna Kaida

Produktdesignerin bei Boldare

Kateryna ist Produktdesignerin und Product Discovery-Evangelistin bei Boldare. Sie unterstützt Kunden und Kundinnen beim Erreichen ihrer Geschäftsziele, indem sie die Bedürfnisse ihrer Kundschaft aufdeckt und versteht. Außerdem hilft sie Unternehmen dabei, riskante Annahmen zu identifizieren und Geschäftsideen mit Hilfe von Product-Discovery-Techniken zu validieren. Zudem ist Kataryna Expertin der von Boldare organisierten Meetup-Reihe Finding Product-Market Fit.

www.boldare.com
Kateryna Kaida auf LinkedIn
https://twitter.com/Boldarecom

V4
VISIONS
WERDE SICHTBAR
ODER VERGESSEN!
SUCHMASCHINEN
OPTIMIERUNG
CONTENT
MARKETING
WEBSITE
ANALYTICS
Lern‘ uns kennen & mach‘ Dein
Online Marketing erfolgreich!
v4-visions.de

391371601 / Adobe Stock

Diese vier Vorteile bietet serverseitiges Tag-Management

von Michael Froment

Die Entwicklung von Adblockern, das Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) und die massive Einschränkung von Third-Party-Cookies hat den Aktionsradius von Daten deutlich verkleinert. Hier kommt serverseitiges Tag-Management ins Spiel. Es eröffnet nicht nur neue technische Möglichkeiten der Datenerfassung in einer restriktiver werdenden digitalen Welt, sondern es bietet Teams auch die Möglichkeit, ihre Daten besser zu pflegen.

Was ist serverseitiges Tag-Management?

Während beim clientseitigen Tagging die Daten zwischen Browser und Nutzer direkt an externe Anbieter gesendet werden, wird beim serverseitigen Tag-Management eine Tracking-Lösung zwischen den Browser des Nutzers und den Endpunkten geschaltet. Die Daten werden mit einer einzigen Anfrage an die Tracking-Lösung geschickt. Dort finden die Aufbereitung der Daten und ihre Verteilung an die verschiedenen Partner statt.

Vier Vorteile auf einen Blick

1. Einfacher hochwertige Daten erfassen

Bei einem serverseitigen Ansatz werden die Daten eines Nutzers oder einer Nutzerin zentral an die Tagging-Lösung geschickt. Diese wiederum bereitet die Informationen auf und leitet sie an Dritte weiter. Mit serverseitigem Tag-Management lassen sich daher im Rahmen der Data Governance die Qualität der Daten überprüfen, Fehler ermitteln und diese mit der gebotenen Sorgfalt korrigieren. Die IP-Adressen können beispielsweise entfernt oder anonymisiert werden, damit sensible personenbezogene Daten nicht an Dritte gehen. Für diese Datenbereinigung stehen weitaus mehr Ressourcen und Kontrollmöglichkeiten zur Verfügung. Dasselbe bei einem clientseitigen Ansatz zu tun ist zwar möglich, belastet aber die Browser-Seite erheblich – dabei kann sich die Customer Experience (CX) stark verschlechtern.

Eine qualitativ hochwertige Erfassung gewährleistet zudem eine einheitliche Datenübertragung und damit einen reibungslosen Betrieb der mit den Daten versorgten Lösungen. Darüber hinaus hilft die serverseitige Verarbeitung von Daten auch dabei, die – aufgrund von Adblockern, der Datenschutz-Grundverordnung (DSGVO) und der Richtlinien nationaler Datenschutzbehörden zur Einholung der Zustimmung – beobachteten Diskrepanzen zwischen analytischen (etwa die durch ein Analysetool gewonnenen Informationen) und transaktionalen Daten (wie die Daten, die beim Kauf in einem Webshop im Backend erfasst werden) zu verringern.

Webbrowser wie Safari und Mozilla setzen auf Intelligent Tracking Prevention (ITP), wodurch Cookies von Drittanbietern blockiert werden und die Nutzeraktivitäten auf Websites sich nicht mehr mit den gängigen Tracking-Technologien verfolgen lassen. Eine ähnliche Situation zeigt sich bei Adblockern. Durch serverseitiges Tag-Management können ITP und Adblocker umgangen und die Websiteaktivitäten der Benutzer*innen trotzdem analysiert werden. Die Datenschutzbestimmungen gelten weiterhin: Um die Daten zu sammeln und zu speichern, wird nach wie vor die Zustimmung der Nutzer*innen benötigt.

2. Teams werden agiler

Teams, die sich erstmals mit einer serverseitigen Lösung beschäftigen, fühlen sich anfangs häufig hilflos, weil das Thema technisch komplex erscheint. Außerdem denken sie nicht daran, dass eine Plattform ihnen helfen kann, die Kontrolle über diese Datenströme zu erlangen.

In der Praxis erleichtert eine serverseitige Plattform viele Datenprozesse, die sich ohne die Hilfe der Server als sehr kompliziert oder sogar als unmöglich erweisen. Bevor die eingehenden Daten an Drittanbieter gesendet werden, können sie zusätzlich mit relevanten Informationen angereichert werden – etwa Daten aus dem CRM, wie Segmentierungs-, Zahlungs- oder Abonnementwerte. Auch Artikelnummern oder Produktdaten lassen sich zu dem Datensatz hinzufügen. Außerdem nützlich: Die Daten können in ihrer Qualität überprüft werden, so lassen sich kaputte oder unvollständige Hits reparieren.

Ein weiterer Vorteil ist das Ende der „Code Freeze“-Zeiten. Die kritischen Momente, in denen nichts mehr auf der Webseite geändert werden kann, um kein Risiko einzugehen, gehören der Vergangenheit an. Bei einem serverseitigen Ansatz erhält der Server immer denselben Datenstrom. Wenn dieser geändert oder korrigiert werden muss, geschieht dies nicht mehr innerhalb des Quellcodes, sondern beim Prozessieren der Daten auf dem Server. Das Ergebnis: Korrekturen können jederzeit erfolgen – egal, ob es sich um die Übertragung zusätzlicher Informationen oder die Änderung von Daten handelt.

Der Übergang zum serverseitigen Tag-Management macht sich im Alltag durch mehr Möglichkeiten und einen spürbaren Agilitätszuwachs bemerkbar.

3. Websites laden schneller

Die Web-Performance ist zu einem Hauptthema in der digitalen Welt geworden, da Websites und mobile Anwendungen den gängigen Anforderungen an Skalierbarkeit und Qualität genügen müssen. Die Leistung steht im Mittelpunkt der Customer Experience: Mehrere Analysen haben ergeben, dass bereits eine Sekunde Verzögerung die Konversionsraten um sieben Prozent beeinträchtigen kann. Das Problem: Nichts ist für ein technisches Team komplexer als eine riesige Menge an „Tags“, die auf der Website stets mitgeladen werden. Denn diese sind nicht immer kompatibel und teilweise sehr unterschiedlich; bisweilen setzen Dritte diese auch ohne alle notwendigen Vorsichtsmaßnahmen ein.

Die Begleiterscheinungen: Langsamere Seitenladezeiten, die durch Schwerfälligkeit und JavaScript-Konflikte entstehen, oder Sicherheitswarnungen mitten in einem Conversion-Tunnel aufgrund eines ungesicherten Tags. In mechanischer Hinsicht schränkt die Reduzierung der Menge an Skripten auf Websites das Risiko einer Verschlechterung der CX ein. So gelingt es technischen Teams, die internen Vorgaben und bisweilen auch die gesetzten Ziele einzuhalten. Mit einer serverseitigen Implementierung lässt sich JavaScript innerhalb der Website auf das Wesentliche beschränken. Dadurch wird es leichter und beansprucht weniger Browser-Ressourcen, sodass dieser den Inhalt schneller bereitstellen kann.

4. Mehr Kontrolle über Sicherheit und Datenschutz

Die digitale Landschaft wandelt sich derzeit auch, um Bedenken in puncto Datenschutz zu reduzieren. Hier kann die serverseitige Technologie einen wichtigen Beitrag liefern. Durch die Verringerung der Anzahl der Tags auf einer Website, die Reduzierung der Datenexposition im Quellcode der Seite und die Kontrolle der Empfänger*innen rüstet sich die digitale Welt mit einer neuen Palette an Funktionen. Dadurch, dass die gesammelten Informationen an einen sicheren Server geschickt werden, haben die Anbieter mehr Kontrolle über die erfassten Daten und darüber, wer sie sehen darf. Nur sie wissen, welche Informationen gesammelt und wohin diese gesendet werden. Vertrauliche Daten etwa können so verschlüsselt an die Empfänger*innen geleitet werden; personenbezogene Daten gelangen nicht in die Hände von externen Parteien. Beim clientseitigen Tagging hingegen können die Drittanbieter alle gewünschten Informationen sammeln. Die verantwortlichen Teams können so die Verwaltung der erfassten Daten auf einer solideren Grundlage neu definieren.

https://www.messerpr.com/fileadmin/user_upload/Vorteile_serverseitiges_Tagging.png (Quelle: Commanders Act)

Zur Erinnerung: Ungenauigkeiten bei der Governance öffnen manchmal Schlupflöcher, etwa beim Piggybacking (Tags, die mehr oder weniger unauffällig andere Tags aufrufen). Die serverseitige Zentralisierung begrenzt diese Risiken.

Bei der Sicherheit gibt es jedoch keine Selbstverständlichkeiten. Nur weil die Interaktionen auf dem Server ablaufen, bedeutet das nicht automatisch mehr Sicherheit. Dies ist erst dann der Fall, wenn die betroffenen Infrastrukturen nach allen Regeln der Kunst geprüft und gesichert werden. Die Sicherheit der serverseitigen Technologie hängt also von den ergriffenen Maßnahmen und den getroffenen Entscheidungen ab.

AUTOR

Michael Froment

Co-Founder und CEO von Commanders Act

Michael Froment ist Co-Founder und CEO von Commanders Act. Er absolvierte einen Master in Ökonometrie sowie einen Master in Marketing und sammelte im Rahmen seiner Studien wertvolle Erfahrungen, durch die er eine Leidenschaft für Daten und deren Verwendung im Marketing entwickelte. Seine Zeit bei AT Internet, einem der führenden Unternehmen im Bereich Web Analyse laut Aussage des Marktforschungsinstituts Forrester Research, trug zu der Entwicklung seiner digitalen Expertise in den Bereichen Tag Management, Attribution sowie Management und Aktivierung von Kundendaten bei. Michael tritt regelmäßig als Experte bei europäischen Konferenzen auf und trägt aktiv zur Erstellung starker Kundenstrategien bei.

https://www.commandersact.com/de/
Michael Froment auf LinkedIn

594956378 / Adobe Stock

Alles, was Sie über die NIS-2-Richtlinie der EU wissen sollten

von Franz Xaver Obermayer

Sind Sie Unternehmer*in mit mindestens 50 Mitarbeitenden und einem Jahresumsatz von 10 Millionen Euro? Dann sind auch Sie verpflichtet, sich an die neue NIS-2-Richtlinie zu halten. Sie kommt in großen Schritten auf uns zu und bringt einige Veränderungen mit sich. Die NIS-2-Richtlinie muss bis spätestens September 2024 umgesetzt werden. Welche Konsequenzen hat das für Betriebe? Worauf müssen Sie als Unternehmer*in jetzt achten und was passiert eigentlich, wenn Sie sich nicht an die neuen Richtlinien halten?

Der Russland-Ukraine-Krieg hat uns allen gezeigt, wie angespannt die Cybersicherheitslage in Deutschland, aber auch in ganz Europa ist. Zudem hat der digitale Wandel ein unglaubliches Tempo angenommen. Der Rat und das Europäische Parlament haben deshalb gehandelt und im Dezember 2022 die NIS-2-Richtlinie verabschiedet. Im Januar dieses Jahres ist sie in Kraft getreten. Nun haben Deutschland und alle anderen EU-Mitgliedstaaten 21 Monate Zeit, um die Regelungen in nationales Recht umzusetzen. Für die betroffenen Unternehmen besteht bereits jetzt Handlungsbedarf.

Die neue Richtlinie NIS-2, The Network and Information Security, löst die alte NIS-Direktive ab. Bisher wurden viele Branchen von den Regelungen weitgehend verschont – nun wird es ernst.

Was für große Unternehmen durch die KRITIS-Verordnung schon lange gilt, kommt jetzt auch auf kleinere Betriebe zu

Mit NIS-2 wird Cybersicherheit und Resilienz nun auch für die breite Masse der Unternehmen in Deutschland zum TOP-Thema. Betroffen sind mittlere Unternehmen mit 50 oder mehr Mitarbeitenden und einem Jahresumsatz von mindestens 10 Millionen Euro sowie große Unternehmen ab 250 Mitarbeitern und einem Jahresumsatz von mindestens 50 Millionen Euro.

Durch die neuen Anforderungen sollen vor allem die Regeln in den 27 EU-Ländern vereinheitlicht werden. Ziel von NIS-2 ist es, kritische Infrastrukturen vor Cyberbedrohungen besser zu schützen und für ein hohes, EU-weites Sicherheitsniveau zu sorgen.

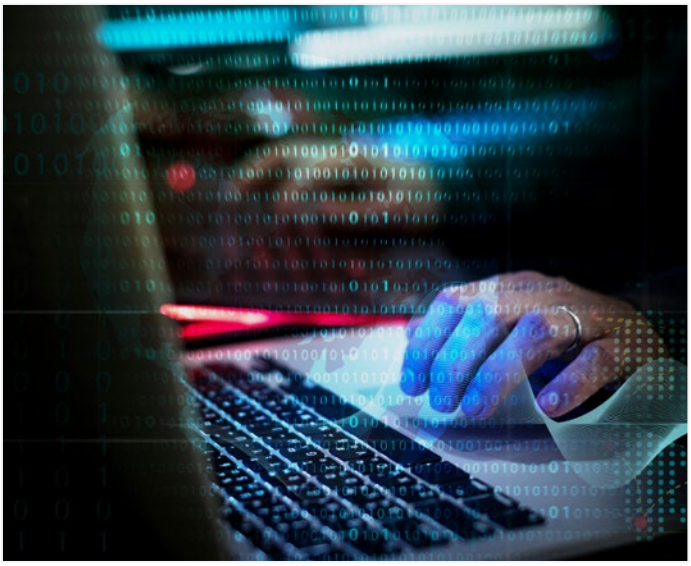
Cyberkriminalität ist schon lange kein Einzelfall mehr

Laut einer Studie des Bundesamtes für Sicherheit in der Informationstechnik war bereits jede*r Vierte der Bevölkerung schon Opfer eines Hacking-Angriffs.

Ein „unsicherer“ Serverraum stellt für die Organisation ein sehr hohes Risiko wie die Gefahren von Angriffen und Schwachstellen dar. Quelle: FOXGroup

Die Cyberkriminellen werden immer einfallsreicher und arbeiten ständig an neuen Methoden, um an wertvolle Daten zu gelangen. Gerade kritische Infrastrukturen und Systeme, die große Bedeutung für das staatliche Gemeinwesen (Energie, Gesundheit, Wasser usw.) haben, sind in den letzten Jahren verstärkt in das Visier der Hacker*innen geraten.

Wer nun neu unter die Richtlinie fällt, sollte schnell handeln. Denn die Beratung sowie die Auswahl passender Technologien und deren Implementierung brauchen Zeit. Viele Firmen, aber auch öffentliche Einrichtungen, haben allerdings Schwierigkeiten, ihre Infrastrukturen adäquat zu schützen, da sie nur eingeschränkte finanzielle und personelle Ressourcen zur Verfügung haben. Einigen ist aber auch die Wichtigkeit von Cybersecurity nicht bewusst und sie gehen fahrlässig mit ihren Daten um. Gerade Betreiber kritischer Infrastrukturen nehmen den Schutz ihrer IT-Infrastruktur trotz zunehmender Gefahren aus dem Cyberraum und anhaltenden Krisen mit Auswirkungen auf die Lieferketten nicht ernst. Dabei entsteht der deutschen Wirtschaft, laut einer Studie des Branchenverbands Bitkom, ein jährlicher Schaden von rund 203 Milliarden Euro.



Cyberkriminelle haben oft leichtes Spiel, Firmendaten abzugreifen und zu verschlüsseln. Quelle: FOXGroup

> „Mit der neuen NIS-2-Richtlinie werden Unternehmen nicht mehr vor die Wahl gestellt, ob sie sich ausreichend gegen Hacker schützen wollen – sie müssen einen Mindeststandard an Sicherheit erfüllen."

Die Mitgliedstaaten haben bis Herbst 2024 Zeit, um NIS-2 in nationales Recht umzusetzen. Fahrlässigkeit kann Unternehmer*innen und Betrieben zukünftig teuer zu stehen kommen. Sie müssen sowohl in die Abwehr als auch in die Wiederherstellung investieren. Wer sich nicht daran hält, dem drohen hohe Bußgelder. Je nach Sektor Maximalstrafen von 7-10 Millionen Euro. Ob auch öffentliche Einrichtungen, die der NIS-2-Richtlinie unliegen, in Deutschland mit den strengen Bußgeldern belegt werden können, bleibt noch abzuwarten.

NIS-1 konnte mit dem rasanten Anstieg der Cyber-Kriminalität nicht mehr mithalten und deshalb hat sich die EU für eine schnelle Ausweitung der Richtlinie entschieden und NIS-2 ins Leben gerufen. Es kommen insgesamt acht neue Sektoren hinzu.

NIS-2 unterscheidet zwischen „Essential Services" und „Important Services"

Die wesentlichen Dienste (Essential Services) werden durch die Sektoren Abwasser, Raumfahrt und die öffentliche Verwaltung ergänzt. Die wichtigen Dienste (Important Services) durch die Sektoren Post und Kurier, Abfallwirtschaft, Chemikalien, Ernährung, Industrie sowie Bildung und Forschung. Besondere Aufmerksamkeit gibt die Richtlinie der digitalen Infrastruktur.

Die EU hat genau festgelegt, welche Cybersecurity-Maßnahmen die Betriebe umsetzen müssen.

Dazu gehören:

- **Policies:** Richtlinien für Risiken und Informationssicherheit
- **Incident Management:** Prävention, Detektion und Bewältigung von Sicherheitsvorfällen
- **Business Continuity:** Backup-Management, Disaster Recovery, Krisenmanagement
- **Supply Chain:** Sicherheit in der Lieferkette
- **Einkauf:** Sicherheit in der Beschaffung von IT und Netzwerk-Systemen
- **Effektivität:** Vorgaben zur Messung von Cyber- und Risikomaßnahmen
- **Kryptographie:** Verschlüsselung wo immer möglich
- **Zugangskontrolle:** Einsatz von Multi-Faktor-Authentifizierung und Single Sign-on
- **Kommunikation:** Einsatz sicherer Sprach-, Video- und Text-Kommunikation

Zugangskontrollen und Sicherheitscodes schützen jedes Unternehmen vor ungebetenen Gästen. Quelle: FOXGroup

Und es kommt noch ein weiterer Punkt hinzu, der Unternehmen vor ernste Herausforderungen stellen wird: Innerhalb von 24 Stunden müssen sie ihre nationale Cybersecurity Behörde unverzüglich über signifikante Störungen, Vorfälle und Sicherheitsbedrohungen ihrer kritischen Dienstleistungen unterrichten, ebenfalls wo möglich die Empfänger*innen (Kunden und Kundinnen) ihrer Dienstleistungen.

Interne Schulung. Quelle: FOXGroup

Mit internen Cybersecurity-Schulungen vorbeugen

NIS-2 verlangt strenge Sicherheitsvorkehrungen, um die ansteigende Cyberkriminalität im Netz einzudämmen. Tatsache ist allerdings auch, dass der größte „Feind“ in den eigenen

Reihen lauert: die Mitarbeitenden. Sie klicken versehentlich auf einen Mail-Anhang und eröffnen so – schnell und einfach – Zugang zu den Daten des Unternehmens. Deshalb ist es wichtig, die eigenen Mitarbeitenden regelmäßig zu schulen und ihnen aufzuzeigen, woran sie sogenannte Phishing-Mails erkennen. Die Schulung der Security Awareness ist ein sehr wichtiger Baustein, der gleichzeitig schnell und kostengünstig umzusetzen ist.

„NIS-2 schreibt Schulungen im Bereich der Cybersicherheit sogar vor."

Fazit

Eine hundertprozentige Sicherheit wird es nie geben. Unternehmen können aber viel tun, um es den Kriminellen so schwer wie möglich zu machen und im Notfall den Betrieb schnell wiederherzustellen. Fehlende Ressourcen sind kein Grund, um den Kopf in den Sand zu stecken – viele Maßnahmen lassen sich mit relativ überschaubarem Aufwand umsetzen.

Fachbegriffe erläutert

NIS	The Network and Information Security
KRITIS	kritische Infrastruktur
Incident Management	Vorfallsmanagement
Business Continuity	Geschäftskontinuität
Desaster Recovery	Datenrettung
Supply Chain	Lieferkette
Multi-Faktor-Authentifizierung	Bei der Multi-Faktor-Authentifizierung handelt es sich um ein Authentifizierungsverfahren, das zwei oder mehr Berechtigungsnachweise (Faktoren) kombiniert.
Phising	Neologismus von fishing, engl. für ‚Angeln'. Man versteht darunter Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben.
Security Awareness	Sicherheitsbewusstsein

AUTOR

Franz Xaver Obermayer

Gründer & Geschäftsführer FOXGroup

Franz Xaver Obermayer arbeitet als Experte für Informationssicherheit und ist in diesem Bereich als Auditor für das Bundesamt für Sicherheit in der Informationstechnik tätig sowie den TÜV Rheinland. Er ist leidenschaftlicher Landwirt und begeisterter ITler. Zugegeben – eine interessante Kombination, die sich aber wunderbar vereinbaren lässt. Sein Wissen als Bio-Landwirt kann er 1:1 in seiner IT-Firma FOXGroup umsetzen. Die FOXGroup ist seit 2021 klimaneutral, es wird ressourcenschonend gearbeitet, produziert und Energie gewonnen.

www.foxgroup.de
Franz Obermayer auf LinkedIn

267042064 / Adobe Stock

Cybersecurity im Mittelstand

von eStrategy Redaktion

Interview mit Marcus Döllerer, Security Engineer bei TechDivision

In einer Welt, in der jedes Unternehmen digital vernetzt ist, ist das Risiko von Cyberangriffen allgegenwärtig. Insbesondere der Mittelstand, der das Rückgrat der Wirtschaft bildet, gerät zunehmend ins Visier von Hackern und Cyberkriminellen – von gezielten Phishing-Attacken über Ransomware bis hin zu komplexen Angriffen auf Unternehmensnetzwerke nehmen die Bedrohungen ständig zu und werden immer raffinierter.

Um mehr über die aktuellen Herausforderungen und bewährten Sicherheitspraktiken im Mittelstandssegment herauszufinden, haben wir uns mit dem erfahrenen Security Engineer Marcus Döllerer unterhalten. Im Gespräch tauchen wir tiefer in die Welt der Cybersecurity ein, versuchen herauszufinden, welche spezifischen Schwachstellen und Herausforderungen mittelständische Unternehmen heutzutage am meisten betreffen, welche Themen Unternehmen als Erstes adressieren sollten und was zu tun ist, wenn der Worst-Case eingetreten ist.

Hallo Marcus, stell´ Dich doch bitte kurz vor. Wer bist und was machst Du?

Mein Name ist Marcus Döllerer und ich bin als Security Engineer bei der TechDivision für den Auf- und Ausbau des Cybersecurity-Bereiches verantwortlich.

Ich beschäftige mich bereits seit meiner Schulzeit sehr intensiv mit IT und habe während meines Informatik-Studiums die Faszination für Cybersecurity entdeckt. Daher war es für mich recht schnell klar, meinen Master genau in diesem Umfeld zu machen.

Bei der TechDivision kümmere ich mich auf der einen Seite darum, das Unternehmen und deren Infrastrukturen gegen Cyberangriffe abzusichern sowie die Mitarbeitenden zu schulen und eine entsprechende Security-Culture innerhalb des Teams zu entwickeln. Auf der anderen Seite helfe ich unseren Kunden und Kundinnen bei der Verbesserung von deren IT-Security durch diverse Beratungsleistungen inkl. Penetrationtesting. Hierzu baue ich derzeit eine eigene Abteilung auf, um diesen Bereich für uns und unsere Kunden weiter zu stärken.

Das Thema Cybersecurity ist inzwischen ja schon fast omnipräsent. Du beschäftigst Dich bereits seit vielen Jahren mit dem Thema. Wie bist Du darauf gekommen und was fasziniert Dich an diesem Bereich?

Wie bereits erwähnt, war ich schon in der Kindheit fasziniert von Computern und Informationstechnologie im Allgemeinen. Dabei hatte ich natürlich immer wieder Berührungspunkte mit IT-Sicherheit – wenn auch nur oberflächlich und ohne es im Detail zu verstehen.

Als Softwareentwickler habe ich mein Hobby zum Beruf gemacht und dabei von Beginn an sehr viel Wert darauf gelegt, sichere Software zu entwickeln.

Ich kann mich auch noch an einen prägenden Moment erinnern, bei dem ich zusammen mit einigen Bekannten ein YouTube-Video von einem Vortrag mit Live-Hacking-Beispielen gesehen habe. Spätestens an dieser Stelle war für mich klar, dass meine Zukunft im Bereich Cybersecurity liegt.

Es gibt ja diesen bekannten Satz „Man fürchtet, was man nicht versteht“. Genau das hat mich angetrieben, tiefer in die Materie einzutauchen und zu verstehen, wie Hacker agieren, was die technischen Grundlagen für Angriffe sind und wie man sich davor schützen kann.
Insbesondere in diesem Umfeld reicht es nicht aus, sich ein oberflächliches Basiswissen anzueignen und dann einfach „blind“ Empfehlungen zu folgen bzw. solche vielleicht selbst zu geben. Man muss verstehen, WARUM etwas angreifbar bzw. nicht angreifbar ist. Hier habe ich über die Jahre ein recht ausgeprägtes Wissen und entsprechende Erfahrungen sammeln können. Was mich zudem fasziniert und motiviert: Man muss jeden Tag dazulernen und sich permanent mit der Materie beschäftigen, die enorm vielschichtig, zum Teil auch äußerst komplex und vor allem sehr dynamisch ist.

Was ist Cybersecurity für Dich und welche Komponenten gehören hier aus Deiner Sicht dazu?

Aus meiner Sicht ist es die richtige Mischung aus Technologien sowie organisatorischen Maßnahmen und Prozessen, die dazu dienen, IT-Infrastrukturen und ihre Nutzer*innen in einer Welt permanenter Bedrohungen hierauf vorzubereiten bzw. zu sensibilisieren. Mit der wichtigste Faktor in diesem ganzen Konglomerat ist der Mensch, der zu möglichen Gefahren und deren Auswirkungen sensibilisiert und geschult werden muss. Dabei ist es aus meiner Sicht enorm wichtig, dass eine Balance zwischen den technologischen Maßnahmen und dem Faktor Mensch geschaffen wird. D. h. es hilft nichts, wenn man die besten Software- und Hardware-Tools zur Gefahren-

abwehr einkauft, die Mitarbeitenden hier aber nicht mitnimmt und entsprechend aufklärt und umgekehrt. Generell halte ich es für essentiell, dass das Thema Cybersecurity so in den Berufsalltag integriert wird, dass damit keine vermeidbaren Hürden und/oder Hemmnisse entstehen. Nur dann kann aus meiner Sicht auch ein wirksamer Schutz aufgebaut werden: die Infrastruktur ist entsprechend vorbereitet bzw. ausgestattet, die Mitarbeitenden sind geschult und entsprechende Schutzmaßnahmen und Regeln sind so ausgelegt, dass sie wirkungsvoll sind, den Arbeitsalltag jedoch nicht unnötig behindern.

Man liest aktuell ja schon fast täglich über immer neue Cyberangriffe und Zwischenfälle. Dabei reicht das Spektrum von kleinen Handwerksunternehmen bis zu Großkonzernen und auch Regierungen. Wie hat sich das Ganze aus Deiner Sicht in den letzten Jahren entwickelt?

In den letzten Jahren hat in diesem Bereich eine enorme Professionalisierung stattgefunden. Ähnlich der Entwicklung von Unternehmen, die sich immer häufiger auf bestimmte Nischen fokussieren, geht der Trend auch im Cybersecurity- bzw. Cybercrime-Umfeld immer mehr in Richtung Spezialisierung wie z. B. die Fokussierung auf den sog. Initial Access – hierunter versteht man den generellen Zugriff auf Unternehmensnetzwerke. Andere nutzen so erhaltene – häufig auch im Darknet gekaufte – Zugänge, um in Unternehmensnetzwerke einzudringen, Daten zu exfiltrieren oder zu verschlüsseln, um dann Erpressungsversuche zu starten. Für Kriminelle ist es inzwischen meist lohnender, sich hier auf einen Teilaspekt zu fokussieren und sich darüber hinaus weiterer „Dienstleister" zu bedienen – auch hier aus rein wirtschaftlichen Überlegungen.

Das Spektrum reicht hier auf Seiten der Opfer von Ein-Personen-Betrieben über KMUs bis hin zu weltweit tätigen Großkonzernen sowie Regierungen. Und auch auf Angreiferseite hat man es immer weniger mit einzelnen Hackern oder sog. Skript-Kiddies zu tun, sondern inzwischen überwiegend mit sehr professionell agierenden Gruppierungen, die teilweise auch auf Anweisung und mit Finanzierung einzelner Staaten agieren – sog. Nation State Actors.

Was sind aus Deiner Sicht die aktuell größten Baustellen gerade im Mittelstand in Bezug auf Cybersecurity?

Sehr häufig ist es im klassischen Mittelstand so, dass die Verantwortung für das Thema Cybersecurity automatisch bei der IT liegt. Nicht jedes Unternehmen hat hier die Mittel und Möglichkeiten, dieser zunehmenden Bedrohung gewachsen zu sein. Hier werden Unternehmen zukünftig inhouse aufstocken und entsprechendes Wissen aufbauen oder sich frühzeitig einen entsprechenden Partner suchen müssen, der in diesem Themenfeld unterstützen kann …

Aus meiner Sicht ist es besonders wichtig, eine umfassende und vor allem realitätsnahe Sicht auf die eigene Angriffsfläche zu haben. Das umfasst die Infrastruktur des Unternehmens inklusive der Mitarbeitenden und aller schützenswerter Assets. Welche Domains, DNS-Einträge, IP-Adressen und Dienste sind eventuell öffentlich auffindbar? Was könnte ein Angreifer noch aus öffentlichen Quellen über mein Unternehmen erfahren? Was könnte denn für einen potenziellen Angreifer interessant sein?

Cybersecurity ist ja ein enorm breites Feld. Was sind aus Deiner Sicht die drei wichtigsten Komponenten/Themen, die Unternehmen hier als erstes angehen und adressieren sollten?

Um das eigene Unternehmen schützen zu können, ist es meiner Ansicht nach essentiell zu wissen, was denn überhaupt geschützt werden muss. Eine Inventur aller Assets ist dafür ein guter Ausgangspunkt. Das Problem ist, dass diese „interne" Ansicht alleine oftmals nicht vollständig ist und daher trügen kann. Wir setzen deshalb darüber hinaus auf eine sogenannte Open Source

Intelligence (OSINT) Analyse, bei welcher wir öffentlich verfügbare Quellen nutzen, um die Sicht eines Angreifers zu simulieren und darüber Assets zu finden, die wir selbst anfangs nicht im Blick hatten. Wir bieten diese Dienstleistung und die dabei gesammelten Erfahrungen mittlerweile auch unseren Kunden und Kundinnen an.

Darüber hinaus würde ich Social Engineering Angriffe, speziell Phishing, als eine der größten Bedrohungen für mittelständische Unternehmen einschätzen. Zwar gibt es technische Ansätze, welche bei der Bekämpfung des Problems unterstützen können. Jedoch ersetzen diese Lösungen keine regelmäßigen Awareness-Schulungen für Mitarbeitende. Wie bei vielen anderen Themen wird auch hier ein hybrider Ansatz aus technischen und organisatorischen Maßnahmen notwendig werden. Für eine nachhaltige Aufklärung der Mitarbeitenden über mögliche Risiken und Gefahren sind regelmäßige Schulungen meiner Meinung nach essentiell.

Zuletzt würde ich nahelegen, früh für einen Ernstfall zu planen. Es ist eine Frage der Zeit, bis der nächste Sicherheitsvorfall eintritt. Egal ob es sich um eine kleine unscheinbare E-Mail oder einen ausgeklügelten Supply-Chain-Angriff handelt: Wenn man auf solche Situationen vorbereitet ist, spart man sich im Ernstfall viel Ärger und kann abends besser schlafen. Ein Incident Response Plan mit Playbooks bzw. Checklisten für mögliche Schadensszenarien ist dabei sehr empfehlenswert.

Gehen wir mal vom Worst-Case aus – ein Unternehmen ist gehackt worden. Wie sollte man hier am besten reagieren und was sind absolutes “No Go´s”?

Das erste, was man machen sollte, ist, sich auf den Worst-Case vorzubereiten. Das nützt natürlich wenig, wenn man jetzt in diesem Moment Opfer eines Cyberangriffs ist. Dennoch will ich es an dieser Stelle nochmal kurz anbringen. Incident Response ist eine Disziplin, welche aus viel Planung besteht. „Planning for failure” ist hier das Stichwort! Hierzu gehört ein sog. Incident Response Plan, der von der Geschäftsführung abgesegnet wurde.
Dabei handelt es sich um einen Maßnahmenplan für IT-Security-Vorfälle, der beschreibt,

PAYMENT

Genießen Sie die freie Auswahl!

Wählen Sie aus über 50 internationalen Acquiring-Partnern Ihre Favoriten.

Ihr Business nimmt auf dem Markt eine einzigartige Stellung ein? Ihre Prozesse und Systeme müssen genau auf Ihr Geschäftsmodell zugeschnitten sein? Dann sollte das auch für Ihre Zahlungsabwicklung gelten. Deshalb speist Sie Computop nicht mit vorportioniertem Payment ab – wählen Sie selbst aus über 50 Acquirern.

Jetzt informieren auf computop.com

Computop
the payment people

welche Schritte von wem unternommen werden müssen, wenn ein Sicherheitsvorfall im Unternehmen auftritt. Ein solider Incident Response Plan soll es Teams ermöglichen, so schnell wie möglich in Aktion zu treten, Angriffe zeitnah abzuwehren und Schäden möglichst schnell zu beseitigen.

Es sollte eine Art Krisenstab bzw. ein Incident Response Team gebildet werden, in dem die weitere Vorgehensweise koordiniert wird und in dem die unterschiedlichen Fäden zusammenlaufen und – sofern intern nicht entsprechendes Cybersecurity Personal sowie ein Legal Counsel zur Verfügung steht – umgehend einen spezialisierten Dienstleister einschalten. Wenn klar ist, dass es sich wirklich um einen Angriff handelt, sollte auch umgehend die Polizei eingeschaltet sowie die rechtliche Meldepflicht beachtet werden. In Bayern steht darüber hinaus die Zentrale Ansprechstelle Cybercrime (ZAC) für die Wirtschaft zur Verfügung.

Wenn man in der Lage ist, eine befallene Datenquelle noch zu isolieren, um eine Ausbreitung im Firmennetzwerk zu verhindern, dann sollte man dies in jedem Fall versuchen. Möglichst schnell den „Stecker zu ziehen" ist in den meisten Fällen keine gute Idee, weil man damit mögliche Hinweise und Spuren vernichten kann und so eventuell nicht mehr nachvollziehen kann, wie der Angriff abgelaufen ist.

Aus meiner Sicht ist es von zentraler Bedeutung, dass man von Beginn an möglichst transparent damit umgeht und aktiv intern und extern kommuniziert. Gut geplante Kommunikation ist während eines Vorfalls besonders wichtig, um unnötige Panik und Unmut unter Mitarbeitenden und Kunden sowie Kundinnen zu vermeiden.

Beim Thema Cybersecurity werden sehr häufig zwei grundlegende Bereiche unterschieden – einmal die Technik und Infrastruktur in Form von Hard- und Software und einmal die soziale Komponente in Form der Mitarbeitenden. Wie bringt man diese beiden Komponenten am besten unter einen Hut und wie viel Aufwand sollte man hier jeweils betreiben?

Eine pauschale Antwort gibt es hier nicht. Idealerweise versucht man, beide Komponenten gleichzeitig zu adressieren und besser miteinander zu vereinen. Es wird häufig argumentiert, dass der Mensch die größte Gefahr darstellt. Aus meiner Sicht können Mitarbeitende, wenn sie entsprechend geschult sind, aber auch eines der größten Assets in der Erkennung von Gefahren darstellen.

Ich habe den Eindruck, dass häufig zu starkes Augenmerk auf technische Lösungen gelegt wird, für Probleme, die oft menschlicher Natur sind. Meist reicht es, die Menschen ordentlich mitzunehmen. Die besten technischen Lösungen bieten keinen 100%igen Schutz, aber sie helfen dabei, es potentiellen Angreifern möglichst schwer zu machen. Ich erachte den Mensch in diesem Kontext aber mindestens genauso wichtig wie die Technologie dahinter.

Wir führen aktuell beispielsweise firmenweit einen neuen Passwort-Manager ein. Im Zuge dieser Einführung erhalten unsere Mitarbeitenden entsprechende Schulungen, mit denen wir auf die Wichtigkeit sicherer Passwörter und den Umgang mit entsprechenden Passwörtern gezielt eingehen und die Features der Software und deren Nutzung erläutern. An diesem Beispiel sieht man ganz gut, dass sich die beiden Komponenten gegenseitig bedingen.

Das Thema Cloud hat zuletzt gerade auch durch die Pandemie nochmals deutlich an Sichtbarkeit und Relevanz zugelegt. In der Vergangenheit war gerade der deutsche Mittelstand häufig recht skeptisch gegenüber der Cloud aufgrund von Sicherheitsbedenken. Wie beurteilst Du das Ganze?

Auch hier ist eine allgemeingültige Aussage, dass die Cloud sicherer oder unsicherer als klassische On-Premise-Software ist, aus meiner Sicht nicht möglich. Die Risiken und Gefahren verändern bzw. verschieben sich hier. Probleme, die im Hosting-Umfeld früher hochgradig relevant waren, sind durch die Cloud kein Thema mehr, da dies durch entsprechende Cloud-Anbieter übernommen wird. Dafür entstehen andere und neue Gefahren. Allgemein bringt „die Cloud" an vielen Stellen eine erhöhte Komplexität, welche wieder Raum für Sicherheitsprobleme mit sich bringt. Ein Beispiel sind die umfangreichen Identity and Access Management (IAM) Rollen, bei denen man viel falsch machen kann.

Cloud Computing ist aus meiner Sicht gekommen um zu bleiben und spätestens mit der Pandemie haben die meisten Unternehmen die Vorzüge der Cloud kennengelernt. Es ist aber sicherlich nicht so, dass durch die Cloud jetzt alle Sicherheitsprobleme vom Tisch sind. Es entstehen neue Gefahren und hier gilt es, sich dieser Entwicklung bewusst zu sein und sich bestmöglich darauf einzustellen.

Welchen Tipp hast Du für Unternehmen, um das Thema Cybersecurity möglichst zielgerichtet anzugehen? Gibt es hier etwas, das man sofort angehen/einführen kann und mit dem man ohne große Aufwände die Sicherheit in seinem Unternehmen verbessern kann?

Das Thema Awareness ist aus meiner Sicht zentral und zwar nicht nur bei den Mitarbeitenden, sondern insbesondere auch auf Geschäftsführungsebene. Die Gefahren werden hier zukünftig sicherlich nicht geringer werden und als Unternehmen muss ich mir – unabhängig von Branche und Größe – dieser Gefahren und den damit verbundenen Auswirkungen bewusst werden und entsprechende Vorkehrungen treffen. Sei es durch sukzessive Thematisierung über das vorhandene Team oder durch Hinzuziehen eines entsprechenden Dienstleisters.

Die Tatsache, dass ein Unternehmen bislang noch nicht betroffen war, bedeutet keinesfalls, dass das Unternehmen für einen Angreifer nicht interessant ist und damit auch keine größere Gefahr besteht. Perspektivisch ist es aus meiner Sicht nur eine Frage der Zeit, bis ein Unternehmen damit konfrontiert wird. Dann sollte man hier bestmöglich vorbereitet sein. Ein Einstieg kann hier beispielsweise die Durchführung eines Penetrationstests durch einen externen Dienstleister sein, mit dem versucht wird, etwaige Schwachstellen herauszufinden, um frühzeitig Absicherungsmaßnahmen durchzuführen, bevor sie von einem bösartigen Angreifer ausgenutzt werden.

Vielen Dank für das Gespräch, Marcus!

Marcus Döllerer

Security Engineer bei TechDivision

INTERVIEWPARTNER

Marcus Döllerer ist Security Engineer bei der TechDivision. Er beschäftigt sich bereits seit seiner Jugend mit Softwareentwicklung und IT-Infrastruktur. Dabei hat er sehr früh seine Leidenschaft für Security-Themen entdeckt. Daher war ein Informatikstudium mit anschließendem Master zum Thema Cybersecurity nur die logische Konsequenz. Bei der TechDivision ist er für die Absicherung der internen Infrastruktur verantwortlich und berät und unterstützt mit seinen Kollegen Unternehmen bei Cybersecurity Themen.

https://www.techdivision.com/leistungen/cyber-security

535447149 / Adobe Stock

Die Bedrohungen nehmen zu

von Rico Barth

Richtig auf Hackerangriffe reagieren

Für manche mag es wie Alarmismus wirken, aber man kann es nicht oft genug sagen: Die Gefahr, Opfer eines Cyberangriffs zu werden, wächst von Jahr zu Jahr. Unternehmen sollten sich nicht mehr die Frage stellen, ob es sie irgendwann mal erwischt, sondern eher wann. Vielerorts lässt die richtige Reaktion auf eine Hackerattacke noch zu wünschen übrig. Und auch in Sachen Vorsorge gibt es bei den meisten Unternehmen noch Luft nach oben. Der vermehrte Einsatz von Open Source-Technologien kann dabei entscheidende Vorteile bringen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat wieder mal besorgniserregende Zahlen geliefert. Allein im Bereich Ransomware sollen 2022 schätzungsweise weltweit über 116 Millionen neue Varianten in Umlauf gekommen sein. Noch düsterer sieht das Fazit des Sicherheitsunternehmens Kaspersky aus. Hier wurden im vergangenen Jahr täglich über 400.000 neue Schadvarianten registriert und das nur in der hauseigenen Antivirensoftware. Die genauen Zahlen lassen sich wahrscheinlich nie ermitteln. Was aber feststeht: Die Situation spitzt sich jährlich zu.

Umso erstaunlicher ist es, mit welcher Gelassenheit viele Unternehmen das Thema behandeln. Besonders in kleinen und mittelständischen Unternehmen herrscht häufig die Meinung vor, dass sie nicht in das Fadenkreuz von Hackern geraten. „Wir machen regelmäßig Sicherheitsupdates, außerdem gibt es bei uns eh nicht viel zu holen", ist oft das Motto. Einen Plan, was nach einem Angriff passieren sollte, gibt es in solchen Betrieben daher erst recht nicht. Dabei übersehen sie, dass es für Hacker nur ein Knopfdruck ist, der zu existenzbedrohenden Schäden führen kann. Wer also denkt, dass es Hacker nur auf globale Konzerne abgesehen haben, irrt.

Paroli statt Panik

Zu den gefährlichsten und leider auch zunehmenden Varianten von Cyberattacken gehören Angriffe mit Ransomware. Im März 2023 hat es beispielsweise einen globalen Angriff dieser Art gegeben, von dem laut BSI alleine in Deutschland eine dreistellige Zahl an Unternehmen betroffen war. Vorfälle mit Ransomware sind besonders heimtückisch, da Hacker damit komplette Computersysteme oder bestimmte Dateien oder Funktionen lahmlegen können und ein Lösegeld für die Freigabe fordern.

Bei den Betroffenen macht sich in den meisten Fällen zunächst Panik breit. Und das ist auch verständlich, denn gerade für kleinere Unternehmen entwickelt sich so schnell eine gefährliche Situation. Ein durchdachtes Handeln ist also besonders wichtig. Bei Ransomware bieten sich verschiedene Lösungsmöglichkeiten an.

Wessen Systeme oder Dateien durch Ransomware blockiert sind, der kann das Problem durchaus durch die eigene IT-Abteilung in den Griff bekommen – ausreichende Kapazitäten und Erfahrung vorausgesetzt. Das Vorgehen der Täter ähnelt sich nämlich häufig und es gibt verschiedene Kriterien, anhand derer sich die Schadsoftware identifizieren lässt. So ist etwa der Text oder der Dateiname der Lösegeldforderung in vielen Fällen gleich oder auch die geforderte Summe oder die Adresse der Erpresser-Mail. Übersichten und den passenden Decryptor gibt es dann einfach im Internet. Wer sich das nicht zutraut, sollte alternativ eine spezialisierte Sicherheitsfirma einschalten.

Bei beiden Optionen ist jedoch nicht garantiert, generell oder zeitnah wieder Zugriff auf seine Dateien zu bekommen. Auch mit der Hilfe von Profis von außerhalb kann es mitunter Wochen oder Monate dauern, bis wieder Normalität einkehrt. Eine dritte Option wäre es deshalb, auf die Forderungen der Erpresser einzugehen. Dieser Schritt sollte aber gut durchdacht sein. Die finanziellen Einbußen können schnell Überhand nehmen, aber auch der mögliche Vertrauensverlust der Kunden und Kundinnen spielt eine große Rolle. In manchen Fällen ist es daher das kleinere Übel, den Hackern nachzugeben. Aber auch dann gibt es keine Garantie, dass alles wieder einwandfrei funktioniert oder man später nicht erneut Opfer einer Attacke wird. Zudem fördert man so die Aktivitäten der Kriminellen – aus ihrer Sicht ist schließlich alles nach Plan gelaufen.

Neben Ransomware gibt es aber auch andere Arten von Cyberattacken, die den Geschäftsbetrieb entscheidend stören können. Sogenannte Social Engineering-Angriffe haben etwa während der Corona-Pandemie stark zugenommen. Hierbei werden die Opfer per Phishing-Mail auf

nachgebaute Webseiten gelockt, die angeblich über aktuelle Themen informieren sollen. Hacker greifen dann die dort eingegebenen Daten der Nutzer ab. In jüngster Zeit geschieht das auch vermehrt durch nachgeahmte Onlineshops, wie das BSI berichtet. Wer seinen Fehler rechtzeitig bemerkt, sollte so schnell wie möglich alle Passwörter ändern. Präventiv hilft hier leider nur, sämtliche Mails, Links und Webseiten genau anzuschauen.

Einen Anstieg hat es auch bei Distributed Denial of Service-Angriffen, kurz DDoS, gegeben. Hierbei überlasten die Hacker Server mit zahllosen Anfragen und nehmen Webseiten so quasi vom Netz. Oft kommen dabei auch Botnetze zum Einsatz, also Zusammenschlüsse von infizierten Computern, mit denen Hacker massive Angriffe starten können. Im Nachhinein lassen sich die eingesetzten IPs sperren, doch die Anzahl ist meistens viel zu groß. Vermeiden lassen sich solche Vorfälle, wenn die eigenen Daten auf mehreren Servern verteilt sind. Das ist zwar zunächst teurer, kann aber vor Totalausfällen schützen.

Nach einem Hackerangriff ist aber nicht nur das Verhalten innerhalb der Firma wichtig, sondern auch die Kommunikation nach außen. Unternehmen sollten ihre Kunden und Kundinnen frühzeitig über den Vorfall informieren, sie auf dem Laufenden halten und mögliche Datenlecks eingestehen. Meistens zeigt die Kundschaft Verständnis und kann ihre eigene Planung anpassen. Steht beispielsweise eine Produktion wegen eines Hackerangriffs still, ist das Problem schon groß genug. Ein geschädigtes Kundenverhältnis sollte dann nicht noch dazukommen.

Prävention mit Open Source

Auch mit allen aktuellen Sicherheitsupdates, einer starken Firewall und aufmerksamem Personal lässt sich die Gefahr eines Hackerangriffs nur reduzieren, aber nie ganz ausschließen. Viele Unternehmen und öffentliche Einrichtungen kommen zudem an dem Thema ISO 27001 und BSI- Grundsicherung und dem Aufbau eines Informationssicherheitsmanagements nicht mehr vorbei – und das ist auch gut so!

520971353 / Adobe Stock

Ein weiteres Mittel, die Sicherheit zu erhöhen, wird von Unternehmen dagegen aber noch häufig übersehen: Der Einsatz von Open Source. Hierbei ist der Quellcode für alle User offen, sie können ihn also einsehen, editieren und nach ihren eigenen Wünschen anpassen. Das klingt zunächst nach einer Einladung für Hacker, doch gerade diese Offenheit macht ihnen das Leben schwer.

Die Stärke von Open Source liegt nämlich in der Teamarbeit. IT-Profis, die eine solche Software beruflich nutzen, können sich in großen Communities austauschen und das System zusammen mit den Entwicklern verbessern. Da viele Menschen hier zusammenkommen, werden mögliche Einfallstore in kürzester Zeit entdeckt und geschlossen. Bei proprietärer, also geschlossener Software, ist das in den meisten Fällen nicht möglich. Und auch auf die zahllosen neuen Schadvarianten lässt sich so deutlich besser reagieren.

Für kleinere und mittlere Unternehmen wäre ein Umstieg auf Open Source nicht nur in puncto Sicherheit interessant, sondern auch in finanzieller Hinsicht. Viele Systeme bieten ein modulares Verkaufsmodell an. Durch den offenen Quellcode lassen sie sich genau auf die verschiedenen Bedürfnisse zuschneiden. Auch hier punktet Open Source also.

Wie sich die Zahlen der Hackerangriffe in den nächsten Jahren entwickeln, müssen wir abwarten. Mit einem Abwärtstrend rechne ich jedenfalls nicht. Ich hoffe aber, dass alle Unternehmen ihre Sicherheitsplanung überdenken, falls sie nicht schon so sicher wie möglich aufgestellt sind. Denn lieber „safe“ als „sorry“ lautet die Devise – auch wenn das Absichern im ersten Schritt aufwändig sein kann. Ein Hackerangriff bereitet deutlich größere Probleme.

AUTOR

Rico Barth

Geschäftsführer KIX Service Software und Vorstandsmitglied Open Source Business Alliance

Rico Barth, Jahrgang 1976, ist einer der digitalen Vorreiter im Lande. 2006 hat er zusammen mit drei Kollegen das Unternehmen KIX Service Software, vormals cape IT, gegründet. Seit 2011 ist er im Vorstand der Open Source Business Alliance. Barth macht mit seinem Unternehmen die IT-Abläufe des deutschen Mittelstands fit für die Zukunft – dafür hat er gemeinsam mit seinen Kollegen sogar den Innovationspreis IT in der Kategorie Open Source auf der CeBIT gewonnen.

https://www.kixdesk.com/
Rico Barth auf LinkedIn
info@kixdexk.com

141328113 / Adobe Stock

Cybersecurity-Maßnahmen im B2B Commerce

von Viktoria Grimm

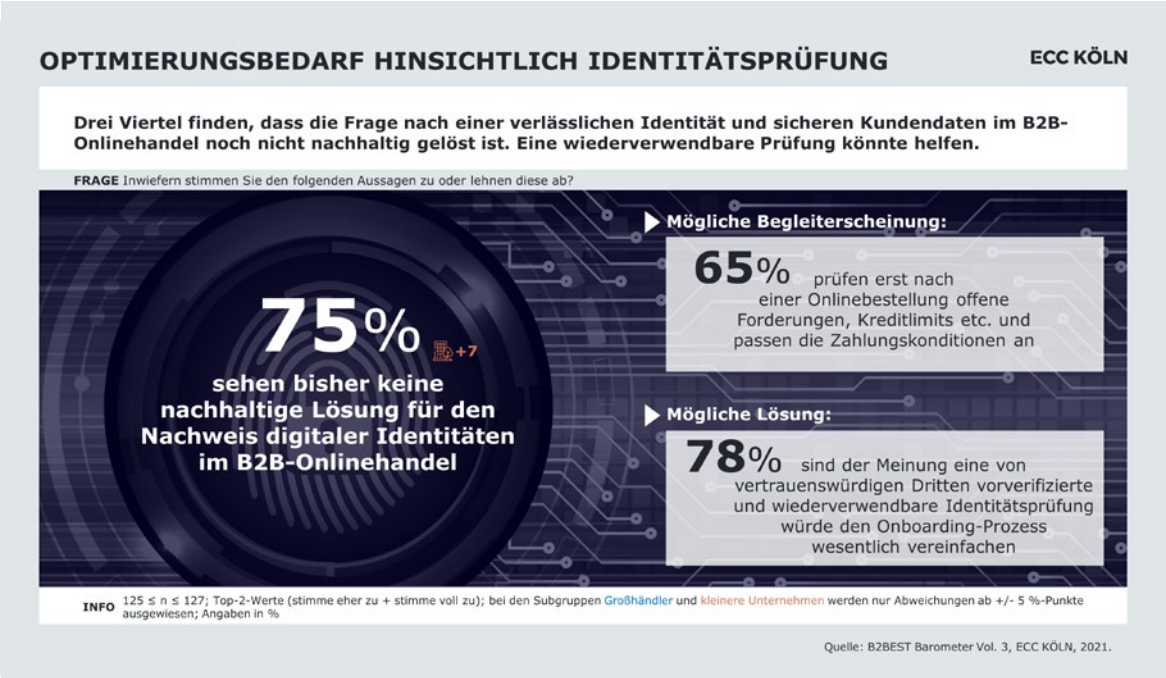
Die positive Entwicklung des E-Commerce im B2B-Handel zeigt immer öfter auch ihre Schattenseiten: Drei Viertel der B2B-Unternehmen sehen einen Anstieg der Betrugsversuche und wollen sich infolgedessen stärker auf den Nachweis digitaler Identitäten konzentrieren. Der Wunsch auf Nutzerseite: Nachhaltige Lösungen für die Identitätsprüfung in Onlineshops.

Betrug wird zunehmend zum Problem im B2B-Handel

Der B2B-Sektor muss sich in vielerlei Hinsicht mit ähnlichen Themen wie der B2C-Sektor beschäftigen. Die fortschreitende Digitalisierung, u. a. befeuert durch die Corona-Pandemie, bringt zwar neue Technologien, aber auch neue Verhaltensmuster beim privaten und beruflichen Einkauf mit sich. Und dies bedeutet auf Händlerseite auch das Auseinandersetzen mit neuen Herausforderungen, insbesondere mit dem Thema Betrug. So zeigt das B2BEST Barometer von ECC KÖLN und Creditreform: 72 % der befragten B2B-Unternehmen verspüren durch den starken Anstieg im Onlinegeschäft auch einen Anstieg an Betrugsversuchen bei Identitätsnachweisen. Der sichere Nachweis digitaler Identitäten ist damit relevanter denn je und die Mehrheit der Unternehmen hat dies frühzeitig erkannt. Risikomanagement und Betrugsprävention sind aufgrund dieser Entwicklungen relevante Themen, mit denen sich vor allem im B2B-Onlinehandel stärker auseinandergesetzt werden muss. Besonders herausfordernd sind die immer professionelleren Methoden der Betrüger*innen, wie beispielsweise gekaufte und gefälschte Account-Zugänge. Aufgrund der Tatsache, dass heutzutage Waren von überall auf der Welt zu jeder Tageszeit bestellt und versandt werden können, sind bereits eingeführte Betrugserkennungssysteme teilweise schon veraltet, da der Einkauf von einer extremen Schnelllebigkeit geprägt ist.

Wunsch nach nachhaltiger Lösung bei höchster Customer Experience

Phishing, Identitätsdiebstahl oder auch der sogenannte Erstattungsbetrug beschäftigen E-Commerce-Betreiber*innen. Das Hauptproblem für den Großteil der befragten Großhändler*innen und Hersteller*innen stellt jedoch der Identitätsdiebstahl dar. Für drei Viertel der Unternehmen fehlt bis heute eine nachhaltige Lösung für den Identitätsnachweis im E-Commerce. Dabei liegt die Lösung für rund 78 % der befragten Großhändler*innen und Hersteller*innen bereits auf der Hand: Eine von vertrauenswürdigen Dritten vorverifizierte und wiederverwendbare Identitätsprüfung. Dies deckt sich auch mit dem Wunsch vieler Endkunden und -kundinnen. Sicherheitsabfragen oder Prüfungsprozesse sollten daher so angenehm wie möglich gestaltet werden, um den Kunden und Kundinnen eine zufriedenstellende Customer Journey zu bieten.

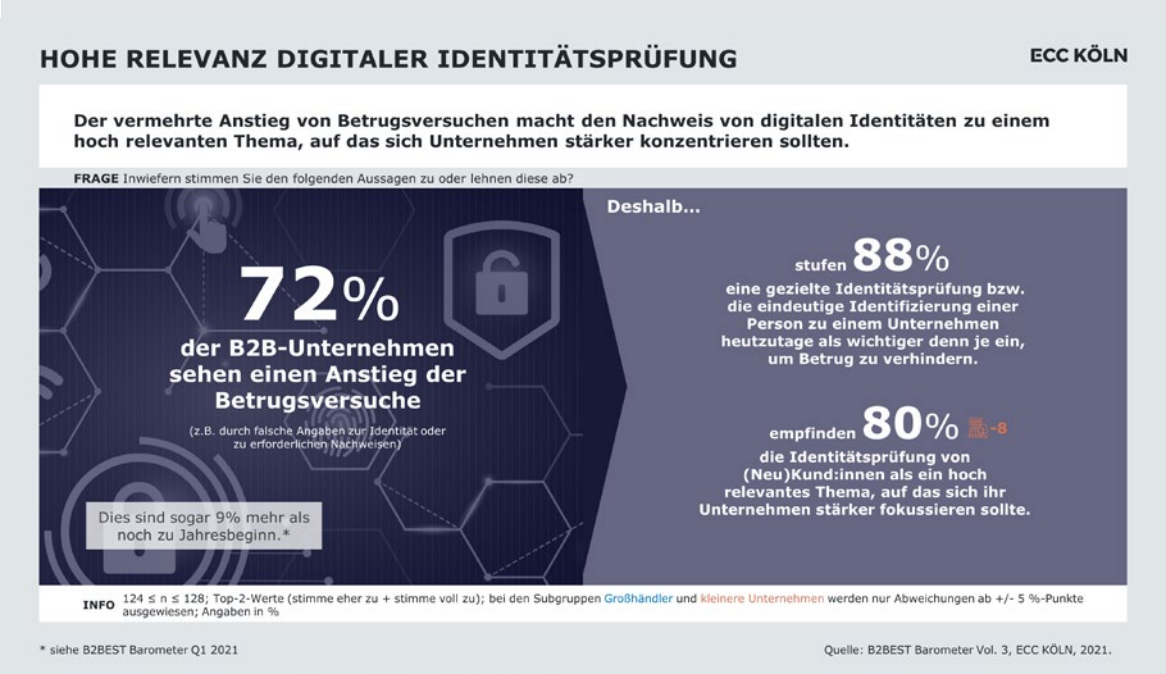


Optimierungsbedarf hinsichtlich Identitätsprüfung

Die überwiegende Mehrheit (84 %) ist der Meinung, dass die hierfür notwendigen Geschäftsprozesse schnell, reibungslos und medienbruchfrei möglich sein sollten, um die Convenience sowie die Customer Experience der Kundschaft zu gewährleisten und positiv zu beeinflussen. Auffällig ist, dass rund 65 % der Befragten erst nach einer Bestellung im Onlineshop prüfen, ob offene Forderungen oder beispielsweise Kreditlimits bei den Kunden oder Kundinnen vorliegen. Erst im nachfolgenden Schritt werden die Zahlungskonditionen angepasst.

Identitätsprüfung von (Neu-)Kunden und Kundinnen hochrelevant

Trotz vieler Herausforderungen: Eine gezielte Identitätsprüfung im Onlinehandel wird von 88 % der B2B-Unternehmen heutzutage als wichtiger denn je eingestuft, um Betrug zu verhindern. Um Neukunden und -kundinnen zu überprüfen, werden aktuell Auskünfte eingeholt (57 %), der persönliche Kontakt gesucht (51 %) sowie Kunden und Kundinnen per Video identifiziert (33 %). Aber auch manuelle Prüfungen von Kundendaten finden in jedem zweiten Unternehmen statt. Damit wird die Identitätsprüfung von (Neu-)Kunden und Kundinnen in 80 % der Unternehmen als hoch relevantes Thema eingestuft. Jedoch fällt auf, dass kleinere Unternehmen sich weniger stark auf den Nachweis digitaler Identitäten fokussieren und weniger Prüfungsformen einsetzen.



Relevanz digitaler Identitätsprüfungen, 2021.

Automatisierung der Registrierungsprozesse als Herausforderung für B2B-Unternehmen

Die Möglichkeit zur Onlineregistrierung für Neukunden und -kundinnen wird im Zuge des wachsenden Onlinegeschäfts von fast jedem B2B-Unternehmen angeboten (93 %). Lediglich in kleineren Unternehmen wird die Onlineregistrierung häufiger verwehrt (12 %). Möglicher Grund hierfür: Die vollständig automatisierte Abwicklung stellt B2B-Unternehmen vor eine Herausforderung. So geben lediglich 18 % der Unternehmen und sogar nur 11 % der kleineren Unternehmen an, Onlineregistrierungen vollständig automatisiert abzuwickeln. In jedem zweiten Unternehmen findet stattdessen immer – sowie in jedem fünften Unternehmen vereinzelt – noch eine manuelle Nachbearbeitung durch den Kundenservice statt.

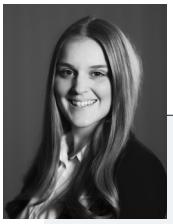
Bei einer Neukundenregistrierung werden am häufigsten Bonitätsinformationen einbezogen oder zusätzliche Gewerbeunterlagen angefordert. Weitere häufig genutzte Maßnahmen im Rahmen einer Neukundenregistrierung sind außerdem der Abgleich mit anderen Verkaufskanälen sowie die Zuordnung zu bestehenden Kundennummern. Externe Datenbanken für die Stammdatenprüfung werden ebenfalls recht häufig genutzt. Auch in diesem Kontext zeigt sich: Kleinere Unternehmen ergreifen generell weniger Maßnahmen bei der Registrierung neuer Kunden und Kundinnen.

Neukundenregistrierung, 2021.

Auffällig ist, dass im Rahmen einer Onlinebestellung sehr häufig interne oder externe Risikoprüfungen, zum Beispiel in Form von Bonitätsprüfungen, durchgeführt werden. Knapp 30 % der Unternehmen setzen sowohl auf interne als auch auf externe Prüfungen und lediglich fast 5 % der befragten Großhändler*innen und Hersteller*innen führen keine Risikoprüfung durch. Aufgrund der heutigen Echtzeitbestellung müssen Risikomaßnahmen ebenso schnell und zeitnah im Hintergrund eines Onlineshops ablaufen, um potenzielle Betrüger*innen fernzuhalten. Die gezielte Prüfung digitaler Identitäten ist hierbei nicht nur zeit-, sondern auch kostenintensiv und stellt Unternehmen vor die Herausforderung, nicht nur gewisse Sicherheitsaspekte zu gewährleisten, sondern den Endnutzer*innen auch eine möglichst angenehme und reibungslose Customer Experience zu ermöglichen. Entsprechend müssen gleich zwei Aspekte von der Händlerseite erfüllt werden: Sicherheit und Bequemlichkeit. Denn wenn eine Neuregistrierung in einem Onlineshop bereits aufwendig und zeitintensiv ist, besteht die Gefahr, dass potenzielle Kunden und Kundinnen diesen Onlineshop gar nicht erst weiter besuchen wollen und im schlimmsten Fall zur Konkurrenz wechseln, welche den Prozess der Neukundenregistrierung eben einfacher und bequemer gestaltet haben.

Fazit

Es lässt sich zusammenfassend festhalten, dass sowohl im B2C- als auch im B2B-Handel Betrugsversuche Unternehmen immer wieder vor eine große Herausforderung stellen. Durch die Einführung neuer Technologien und die dadurch entstehenden neuen Möglichkeiten im E-Commerce-Vertrieb müssen Händler*innen ihre Sicherheitsmaßnahmen an neue Standards anpassen.



AUTORIN

Viktoria Grimm

Junior Projektmanagerin am IFH KÖLN

Viktoria Grimm ist seit März 2022 am IFH KÖLN tätig und fokussiert sich auf Projekte rund um den B2B-Bereich und das Thema Payment. Dabei stehen insbesondere kleine und mittelständische Unternehmen im Fokus mit Fragen zur internen Transformation bis hin zur digitalen Außenwahrnehmung.

https://www.ifhkoeln.de/
Viktoria Grimm auf LinkedIn

592541787 / Adobe Stock

Mitarbeiter-Manipulation

von Sebastian Gerstl

Social Engineering ist viel älter als Cybersecurity und setzt beim Menschen an

In Zeiten von Digitalisierung, Technisierung und IT in Unternehmen wird immer wieder gewarnt, dass Cybersecurity wichtig sei. Ein Aspekt wird dabei aber sehr häufig vernachlässigt. Egal wie gut die Antivirensoftware, die Logins oder die Firewalls sind, eines der schwächsten Glieder in der gesamten Verteidigungskette ist und bleibt der Mensch. Über Social Engineering kommen Cyberangreifer sehr häufig an sensible Daten und in das Netzwerk hinein. Doch worum handelt es sich bei Social Engineering und warum ist das nach wie vor so gefährlich?

Sebastian Gerstl vom Heise Meets Podcast hat sich hierzu mit dem ausgewiesenen Experten Dr. Christian Schunck, Senior Scientist beim Fraunhofer Institut für Arbeitswirtschaft und Organisation (IAO), unterhalten.

Sebastian Gerstl (SG): Social Engineering als Aspekt der Cybersecurity wird ja oft massiv unterschätzt. Keine Firewall, keine Antivirensoftware kann da verlässlich davor schützen. Aber worum handelt es sich jetzt konkret dabei, wenn wir von Social Engineering sprechen?

Dr. Christian Schunck (Dr. CS): Social Engineering ist im Grunde viel älter als Cybersecurity und setzt bei Menschen an. Als Menschen sind wir soziale Wesen, deswegen auch Social Engineering. Wir haben uns typische menschliche Verhaltensweisen angeeignet, die es uns erlauben, als Wesen in einer Gesellschaft gut zu funktionieren, da reinzupassen, Zugehörigkeitsgefühle zu entwickeln und Menschen zu helfen. Gerade diese sozialen Verhaltensweisen werden dann angesprochen, um Menschen zu beeinflussen, bestimmte Entscheidungen zu treffen oder auch Menschen gezielt zu manipulieren.

SG: Was für Mechanismen kommen dabei zum Einsatz? Also wo setzt dieses Social Engineering denn konkret an?

Dr. CS: Es ist so, dass diese sozialen Verhaltensweisen und das Beeinflussen einer Entscheidung ja erst mal gar nicht im Cybersecurity Kontext so interessant sind. Wenn ich einfach sage oder sagen würde, wir möchten die Entscheidungsfindung von Menschen beeinflussen, dann würden sie vielleicht an Marketing denken, an Vertrieb, an Verkauf. Und aus diesem Bereich kommt auch die Forschung zum Thema Social Engineering. Da wurde untersucht, welche Mechanismen funktionieren denn, damit ich Menschen dazu bewegen kann, etwas zu kaufen oder etwas zu tun. Und welche Mechanismen sind das? Das sind Mechanismen wie Hilfsbereitschaft.

Wir sind als Menschen erst mal gewillt, anderen Mitmenschen zu helfen. Nun muss ich diese Hilfsbereitschaft vielleicht ein bisschen anstupsen. Und dazu gibt es zwei Techniken, die letztlich dazu dienen, die Wahrscheinlichkeit, dass man die richtige Entscheidung im Sinne dessen, der die Entscheidung herbeiführen möchte, trifft. Um diese Entscheidungsfindung anzutreiben, wird dann zum Beispiel darauf gesetzt, dass wir Menschen einen Gefallen gerne honorieren wollen.

Also wenn mir jemand etwas gibt, bin ich viel geneigter, dem anderen Menschen auch in irgendeiner Form einen Gefallen zu erwidern. Das sehen Sie im Supermarkt. Da wird Ihnen ein kleines Stückchen Käse angeboten in der Hoffnung, dass Sie dann das große Stück Käse kaufen. Das kann man dann beim Social Engineering anwenden, um Menschen dazu zu bewegen, zu helfen oder auf einen Angriff reinzufallen. Es gibt Beispiele, wo zum Beispiel Angestellten ein Schokoriegel gegeben wurde und die daraufhin ihr Passwort gesagt haben. Das funktioniert natürlich dann nicht ganz so plump. Sie können sich vielleicht vorstellen, da stehen Leute vor dem Geschäft und teilen Schokolade aus und wünschen erstmal einen schönen Arbeitstag und sagen: “ Jetzt hätten wir noch eine kleine Frage. Wir machen eine Umfrage zur Passwortsicherheit und möchten mal wissen, welche Arten Passwörter denn benutzt werden können. Können Sie uns vielleicht mal einige von Ihnen mitteilen?”

SG: Das hört sich jetzt aber nach einem ziemlich extremen Beispiel an!

Dr. CS: Ja, das ist ein extremes Beispiel, aber es hat funktioniert. Und diese Mechanismen, die funktionieren extrem gut. In der Wirtschaftsforschung oder der Verhaltenspsychologie sind diese Prinzipien dafür bekannt, dass sie die Wahrscheinlichkeit, dass Menschen entsprechend reagieren, extrem steigern. Das klingt jetzt vielleicht plump, wie das Beispiel mit dem Schokoriegel, aber das geht natürlich auch subtiler und funktioniert dann immer noch.

SG: Etwas, was man in der letzten Zeit sehr häufig hört, also auch in der Medienlandschaft, ist der sogenannte CEO-Fraud: Ein Angreifer bringt es fertig, eine E-Mail so zu manipulieren, dass sie so aussieht, als würde sie vom Geschäftsführer des Unternehmens kommen. Wo setzt dieser CEO-Fraud an und wie funktioniert das Ganze?

Dr. CS: Der CEO-Fraud setzt da an, dass der CEO als eine Autorität wahrgenommen wird, dessen Anweisungen man befolgen muss. Und das ist nun auch wieder erstmal eine gewisse wünschenswerte Verhaltensweise im Unternehmen. Die Unternehmen möchten natürlich schon, dass Aufträge von Vorgesetzten auch ausgeführt werden. Das ist also ein grundsätzlich gewünschtes Verhalten und das wird von Angreifern dann ausgenutzt. Beim CEO-Fraud wird dann z. B. ein Angestellter oder eine Angestellte meist per E-Mail aufgefordert, für eine geheime Unternehmensübernahme Geld ins Ausland zu überweisen. Diese Person wird dann vielleicht noch gelobt, dass sie als besonders zuverlässig bekannt ist und zur absoluten Geheimhaltung verpflichtet ist, weil diese Übernahme hochsensibel ist und erst mal erfolgen muss, bevor man darüber sprechen kann. Deswegen darf die Person sich auch nicht an Kollegen wenden. Und so wird dann diese Person unter dem Prinzip der Autorität vielleicht noch ein bisschen geschmeichelt, aber auch extrem unter Druck gesetzt im Sinne von Geheimhaltung, nicht mit Kollegen reden. Natürlich muss alles auch wahnsinnig schnell erfolgen, denn sonst geht die Transaktion den Bach runter und dann ist der Chef unglücklich. Und ja, das funktioniert erstaunlich gut. Die Schäden in Deutschland mit diesem Trick dürften die 100-Millionen-Grenze bereits überschritten haben, weil es hier auch immer um große Summen geht. Wenn es klappt, dann werden schnell mal mehrere hunderttausend Euro überwiesen.

Sofern man als Firmenchef seine Mitarbeiter hierauf nicht vorbereitet – gerade die, die in der Lage sind, solche Transaktionen zu machen – ist natürlich die Wahrscheinlichkeit, dass solche Angriffe erfolgreich durchgeführt werden können, relativ hoch.

SG: Speziell in dem Aspekt CEO-Fraud kommen ja gleich mehrere Dinge ins Spiel, die so auch mit der Gemütswelt des Angegriffenen spielen. Da ist zum einen natürlich der Respekt. Der Chef ist die Autorität, dem folgt man. Dann ist da vielleicht auch so ein bisschen Furcht mit dabei. Man ist es in der Unternehmensstruktur meist ja nicht gewohnt, dass man dem Chef widerspricht oder ihm gegenüber entsprechende Zweifel äußert.

Dr. CS: Man geht ja davon aus, wenn das direkt vom Chef kommt, dann wird das schon seine Richtigkeit haben. Dann spielt das Thema Stolz natürlich auch eine Rolle. Man wird als Vertrauensperson herangezogen. Man kann sich da jetzt bewähren und beweisen oder man ist einfach so dermaßen im Stress und unter Arbeitsdruck, dass das reinkommt und man will das gar nicht hinterfragen. Man will das gar nicht aufhalten. Man will sich auch selber nicht lange damit beschäftigen und gibt das gleich mal wieder weiter. Also da kommen mehrere Aspekte ins Spiel, die so im gewöhnlichen Arbeitsalltag eigentlich permanent vorherrschen.

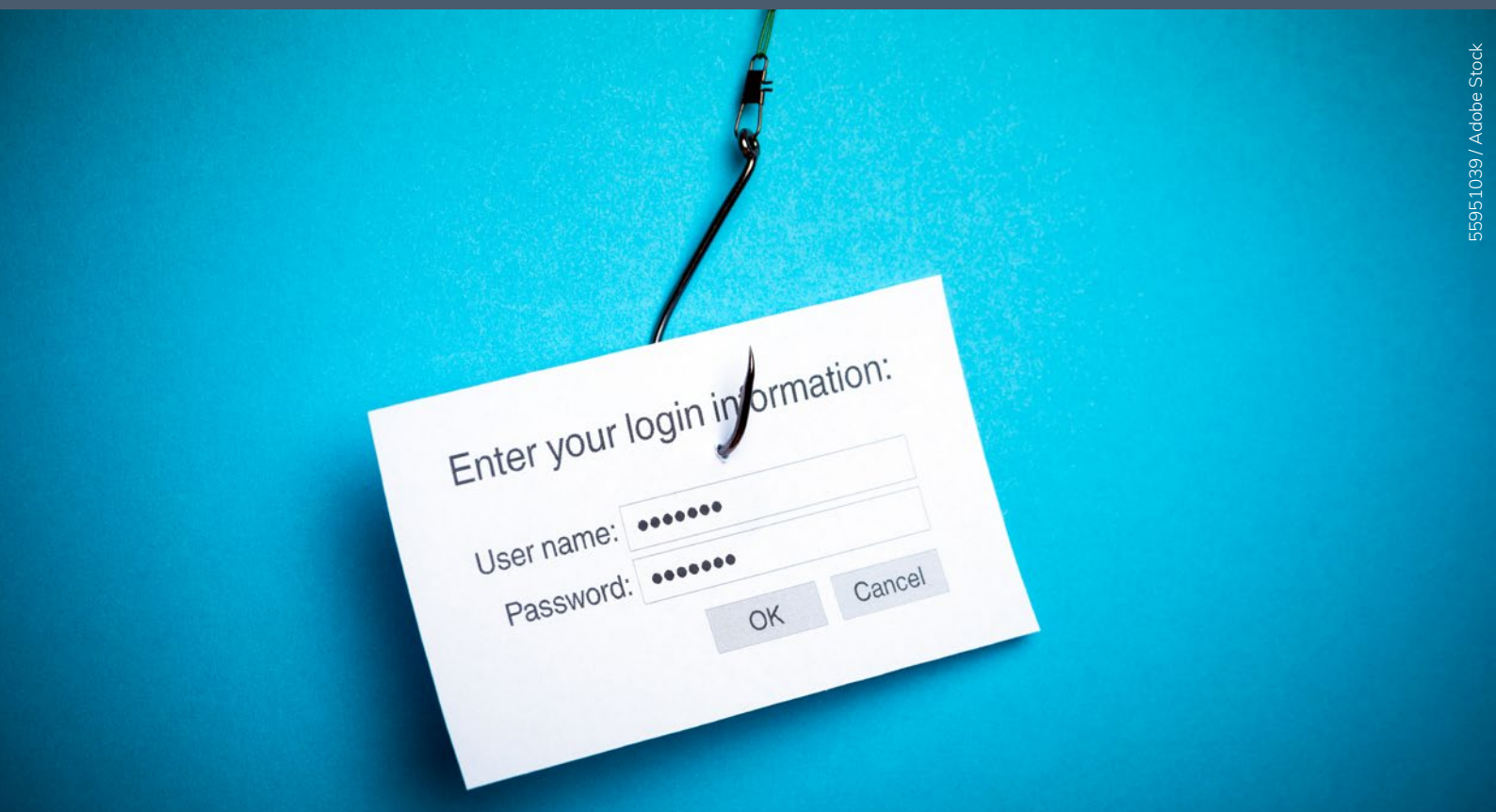
Genau das wird dann ausgenutzt. Um dagegen arbeiten zu können oder um einen Teil dieser wünschenswerten Arbeitsweisen zu erhalten, aber gleichzeitig zu verhindern, dass sie ausgenutzt werden, muss man im Unternehmen dafür sorgen, dass bestimmte Regeln eingehalten werden. Wenn also für manche Transaktionen das Vier-Augen-Prinzip notwendig ist und die Angestellten das wirklich wissen – das Prinzip muss befolgt werden und zwar immer und ausnahmslos – dann trifft so eine Bitte, das zu ignorieren, natürlich erst mal auf größere innere Widerstände, als wenn es das Prinzip in dem Unternehmen zwar gibt, aber es immer wieder mal auch auf Anordnung vom Chef verletzt wird. Also da gehört schon dazu, dass man erst mal das Personal schult und auf solche Arten von Angriffen aufmerksam macht. Das zweite ist, dass man

Regeln, die notwendig sind, z. B. solche Transaktionen nicht ohne Vier-Augen-Prinzip durchzuführen, auch wirklich konsequent einhält.

SG: Jetzt sind wir sehr lange auf den CEO-Fraud eingegangen. Welche anderen typischen Angriffe gibt es für gewöhnlich noch?

Dr. CS: Die bekanntesten sind sicherlich die Phishing-E-Mails. Die gibt es in ganz vielen Varianten. Da werden Mitarbeiter beispielsweise aufgefordert, irgendwelche Webseiten zu besuchen oder Dateien zu öffnen. Nach dem Motto: „Hallo, hier ist die IT. Wir wollen die Passwörter ändern. Bitte gehen Sie auf diese sehr täuschend echt nachgemachte Webseite des Unternehmens und geben Sie hier mal Ihr Passwort ein." Das kann natürlich auch andere Formen haben. Es kann das verlockende Jobangebot sein, wo sich das Gehalt verdoppelt und es zusätzlich noch tolle Benefits gibt – wie zum Beispiel ein E-Auto oder einen E-Scooter. Und dann wird man aufgefordert, eine angehängte Datei zu öffnen. Oder man wird über LinkedIn angeschrieben. Man chattet über LinkedIn und irgendwann kommt eine schmeichelhafte E-Mail. Da steht dann beispielsweise, dass der Inhalt nur durch Aktivieren der Makros angezeigt werden kann. In einem solchen Fall kann die Versuchung dann schon groß sein.

Ein anderer Angriffsvektor, der sehr gut funktioniert, ist das gute alte Telefon. Da rufen Leute an, die sagen, sie seien aus der IT oder aus dem HR etc. In großen Firmen, wo man die Leute vielleicht auch nicht persönlich kennt, können sie mit allen möglichen Anfragen kommen. Da kann es sein, dass nach anderen Mitarbeitern oder nach Informationen zu anderen Mitarbeitern gefragt wird. Das klingt dann vielleicht auch harmlos, weil vielleicht nur nach einem Namen oder einer Personalnummer gefragt wird. Oft lehnt sich der Mitarbeiter nach einem solchen Anruf erstmal zurück und denkt an nichts Böses. Allerdings ist es oft so, dass diese Angreifer mehrstufig vorgehen und vier, fünf Leute im Unternehmen anrufen und so langsam die Information aggregieren, um dann vielleicht später ganz gezielt auf das eigentliche Opfer eingehen können. Insbesondere vermeintliche Anrufe der IT können sehr vielfältige Formen haben z. B. „Gehen Sie auf diese Webseite oder öffnen Sie mal die Kommandozeile und geben Sie Folgendes ein …"



55951039 / Adobe Stock

Ein anderes Ziel geht dann eher in Richtung Industrie-Spionage. Also, dass man wirklich versucht, an Betriebsgeheimnisse heranzukommen. An die neue Marketingkampagne, die geplant ist und an Unterlagen dazu oder an Konstruktionszeichnungen für irgendwelche neuen Komponenten. Auch da werden immer diese Prinzipien genutzt, um zu appellieren. Also zum Beispiel: „Ihr Kollege hat mir auch schon geholfen in einer ähnlichen Situation" und man lässt noch den Namen fallen, den man auf der Webseite gefunden hat. Oder man sucht einen unzufriedenen Mitarbeiter, der irgendwie dann so das Gefühl hat, jetzt kann er seinem Unternehmen eins auswischen – die Variante gibt es wahrscheinlich auch.

SG: Sie haben ja erwähnt, dass sehr viel über das Telefon auch heute noch geschieht. Das ist ja alles andere als ein neuer Weg. Ich meine, selbst in den 70er Jahren hat ein so berüchtigter Hacker wie Kevin Mitnick damals schon gesagt, dass häufig sein erster Weg über das Telefon ging.

Dr. CS: Auf jeden Fall! Ich würde fast sagen, es ist ziemlich alt und doch vertraut. Man versucht durch den Einsatz irgendeiner Technik Menschen in der Entscheidungsfindung zu beeinflussen – das sitzt wirklich tief. Da wundert man sich doch, wie dann anhand der ganzen fortschrittlichen Technologie und IT, die wir haben, so eine uralte Methode in der modernen Zeit immer noch so gefährlich sein kann. Man muss natürlich auch sagen, die Technik ist auch nach wie vor nicht perfekt und wahrscheinlich wird sie es auch nie sein, aber sie ist halt mittlerweile schon sehr, sehr, sehr, sehr gut.

Wenn man nicht wirklich ein spezielles Ziel hat, dann ist es einfach ein Spiel der Wahrscheinlichkeiten. Was funktioniert am besten? Und da kann ich natürlich irgendwelche Ports scannen oder nach bekannten Schwachstellen suchen. Wenn sie frisch sind, finde ich sie hier und da und dann kann ich auch die Technik überwinden, wenn diese Schwachstellen nicht rechtzeitig gepatcht wurden. Was durchaus sein kann. Wenn das Zero-Day-Exploits sind, kann ich damit ganz gut weiterkommen. Insofern kann man dann die Technik ausnutzen. Aber der Standard ist sehr hoch und es wird auch immer schwieriger.

SG: Gleichzeitig ist es ja auch so: In Zeiten immer fortschrittlicher oder immer komplizierter erscheinender IT hat der Anwender selber wahrscheinlich nicht so viel Ahnung oder Durchblick und verlässt sich dann darauf, dass wenn etwas von der IT oder von Human Resources kommt, dies schon seine Richtigkeit haben wird.

Dr. CS: Auf jeden Fall spielt das eine große Rolle. Letztlich haben wir unsere Interaktionen in der realen Welt gelernt. So ein flacher Bildschirm vor uns mit irgendwelchen Fenstern, die sich da öffnen, und Sachen, die da im Hintergrund passieren, ist für viele Nicht-ITler einfach eine fremde Welt. Davon müssen sie nicht viel verstehen und vielleicht möchten sie es auch nicht verstehen, um ihren Job gut zu erledigen. Insofern ist es auch schwierig, dafür Intuition und Verständnis zu entwickeln. Auch diese mangelnde Intuition und dieses mangelnde Verständnis kann man dann wieder ausnutzen, weil Angegriffene sich vielleicht nicht immer bewusst sind, was jetzt eine bestimmte Aktion von ihnen wirklich bewirkt.

An dieser Stelle ist es besser, man schult Mitarbeiter so, dass auch da die Wahrscheinlichkeit verringert wird, dass solche Sachen erfolgreich sind. Und letztlich – da denke ich ähnlich wie Marketingleute – ist es ein Spiel der Wahrscheinlichkeiten, dass etwas funktioniert und nicht, dass es nicht funktioniert. Bei der Technik machen wir das schon ziemlich gut. Bei Menschen sehe ich persönlich noch Entwicklungspotenzial.

SG: Auch durch KI werden die Gefahren im Bereich Cybersecurity immer größer und man kann jetzt auch schlecht eine „Misstraue-Allem-Und-Jedem"-Strategie fahren. Wie sollte man an solche Problematiken rangehen? Liegt das vielleicht auch an der Unternehmensstruktur? Oder werden Angestellte mit Security Trainings auch eher überfordert, also, dass sie sich zu sehr auf die technische Seite verlassen und dann auf der sozialen Ebene leichter angreifbar werden? Wo kann man da ansetzen? Wo liegen die größten Gefahren und die Baustellen, die innerhalb eines Unternehmens adressiert werden müssten, um solche Gefahren zumindest zu minimieren?

Dr. CS: Grundsätzlich ist es so wie bei der IT-Sicherheit auch. Man muss sich erst mal als Unternehmen fragen, was sind meine Schlüsselfähigkeiten, was sind meine Schlüssel-Assets, die ich habe, was muss ich schützen. Darauf aufbauend muss man dann überlegen, wie man dies am besten schafft: auf technischer Ebene und auf Ebene der Mitarbeiter.

Wenn wir uns Social Engineering angucken, ist es hauptsächlich auf Ebene der Mitarbeiter. Da kann ich dann – wenn ich weiß, was ich schützen möchte – auch prüfen, welche Mitarbeiter und Mitarbeitergruppe hier Schlüsselrollen einnehmen. Dann kann ich beginnen, diese Gruppen gezielt zu schulen. Sie haben die Organisationsstrukturen angesprochen. Hier sollte ich mir sehr genau anschauen, wie meine Organisation läuft und tickt – welche Kultur haben wir, wie unterstützt die Organisationsstruktur unser Geschäftsmodell? Wenn man das verstanden hat, kann man dann einen Schritt zurückgehen sowie analysieren und sich fragen: Mit welchen dieser Werkzeuge eines Social Engineers kann ich gerade hier besonders gut vorgehen, wo ist die Wahrscheinlichkeit wieder höher, dass ein Angriff funktioniert oder nicht? Dann kann man entsprechende Maßnahmen treffen. Darauf muss ich meine Mitarbeiter ganz besonders vorbereiten. Der erste Schritt ist eine Analyse und im zweiten Schritt kann man sich dann überlegen, was man den Mitarbeitern beibringen muss.

Und letztlich sehe ich das so, dass gerade der Bereich Social Engineering nicht nur in der IT-Sicherheit eine Rolle spielt, sondern überhaupt im ganzen sozialen Miteinander. Wie gesagt, diese Techniken werden auch im Marketing ausgenutzt, z. B. wenn ihnen jemand ein Auto verkaufen möchte. Insofern ist da eigentlich auch ein Mehrwert dabei, Mitarbeitern das mal zu zeigen und vielleicht auch ein Stück weit erleben zu lassen. Daher könnten Unternehmen dadurch, dass sie in diesem Bereich Mitarbeiter trainieren, wirklich auch für Mitarbeiter einen Mehrwert schaffen, der weit über die IT-Sicherheit des Unternehmens hinausgeht.

SG: Das klingt ja wirklich so wie ein in den 1930er Jahren geschriebenes Buch „How to Win Friends and Influence People" von Dale Carnegie – auch heute noch eine sehr empfehlenswerte Standardlektüre für jeden Angestellten in einem Unternehmen.

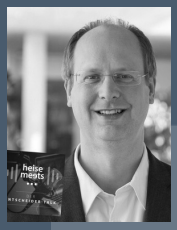
Dr. CS: Ja, das klingt fast so. Aber das Fraunhofer IAO selber bietet ja auch direkt Schulungen und Kurse zum Thema Social Engineering an, damit man sich da so ein bisschen vorbereitet und wappnet. Wir machen das auf unterschiedliche Art und Weise. Teilweise können uns Unternehmen einladen, dann machen wir das für die Mitarbeiter des Unternehmens oder ausgewählte Mitarbeitergruppen. Da kann man auch erst schauen, für welche Gruppen das vielleicht am interessantesten ist. Auch bieten wir das bei uns am Fraunhofer IAO an, wo Unternehmen einige Mitarbeiter zu uns schicken können. Worum es da geht, ist auch so ein bisschen das Erleben. Wie fühlt man sich in so einer Situation? Vielleicht auch die Techniken selber mal ein bisschen ausprobieren.

Auf der anderen Seite ist das Ziel, ein Bauchgefühl zu entwickeln, welches einem ermöglicht – wenn man einen Fehler gemacht hat – möglichst schnell noch zu reagieren und die IT zu informieren. Natürlich geht es in erster Linie darum, mögliche Angriffe gleich abzuwehren, aber auch darum z. B. im Nachhinein noch schnell aktiv zu werden, weil man sowohl emotional als auch intellektuell darauf vorbereitet ist, dass sowas passieren kann. Es geht auch darum, die Techniken ein bisschen kennenzulernen – was Open Source Intelligence ist, wie sich Social Ingenieure oder Angreifer wirklich vorbereiten können auf ein bestimmtes Gespräch. Man kann auch aus öffentlich verfügbaren Informationen sehr viel rausholen. Auf sowas gehen wir dann auch ein, um einfach Menschen zu zeigen, wie gut Leute vorbereitet sein können, wenn sie vorbereitet sein wollen.

SG: Wie heißt es doch so schön: Vertrauen ist gut, ein gutes Bauchgefühl und sicherheitshalber nochmal nachhaken und nachfragen an dritter Stelle ist besser. Auch wenn die Zeit drückt und man sich besonders eingeschüchtert oder besonders gebauchpinselt fühlt, es lohnt sich immer, nochmal an entsprechender Stelle innerhalb des eigenen Unternehmens nachzuhaken. Vielen herzlichen Dank für Ihre Ausführungen und Einblicke.

Das Interview von Sebastian Gerstl mit Dr. Christian Schunck, Senior Scientist Fraunhofer IAO, stammt aus dem Heise Meets Podcast vom 10.05.2023 und wurde eStrategy von Heise Meets zur Verfügung gestellt.

INTERVIEWPARTNER



Dr. Christian Schunck

Senior Scientist Fraunhofer IAO

Dr. Christian Schunck hat Physik studiert und ist seit vielen Jahren in der Forschung tätig. Sein Beruf führte ihn in die USA (Berkeley, MIT) sowie nach Italien (Universität Rom). Derzeit arbeitet er beim Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO) in Stuttgart, wo er sich mit digitalem Identitätsmanagement beschäftigt. Dazu gehört auch das Social Engineering, über das Cybergangster immer wieder in Netzwerke von Unternehmen eindringen und somit an sensible Daten gelangen.

463624519 / Adobe Stock

Trends im Recruiting

von Antonia Breitenfellner

Was sind die aktuellen Entwicklungen und wie können Unternehmen sie nutzen?

Die Suche nach den besten Talenten war noch nie eine leichte Aufgabe für Unternehmen. Aber in einer Welt, die von Digitalisierung und demografischem Wandel geprägt ist, stehen Recruiter vor ganz neuen Herausforderungen. Die Konkurrenz um qualifizierte Mitarbeitende ist stärker als je zuvor und Unternehmen müssen sich auf dem neuesten Stand der Recruiting-Trends halten, um im Kampf um zukünftige Arbeitskräfte erfolgreich zu sein.

Der folgende Beitrag konkretisiert die Recruiting-Maßnahmen, die Unternehmen anwenden sollten, um die vielversprechendsten Talente für sich zu gewinnen.

Personalisierte Stellenanzeigen

Ein Trend im Recruiting ist die Personalisierung von Stellenanzeigen. Statt herkömmlichen und generischen Jobbeschreibungen sollten Unternehmen individuelle Stellenanzeigen für jede Position erstellen. Hierbei müssen die spezifischen Anforderungen der Stelle sowie die Bedürfnisse der Kandidaten und Kandidatinnen berücksichtigt werden. Personalisierte Stellenanzeigen haben gezeigt, dass Bewerber*innen sich dadurch angesprochen fühlten und dazu ermutigt wurden, sich für die Position zu bewerben. Individuelle Anzeigen tragen zudem dazu bei, dass Bewerber*innen sich besser auf die Anforderungen der Stelle vorbereiten können und demnach besser geeignet sind.

Die Plattform Softgarden, die Unternehmen beim Arbeitskräftemanagement und der Personalbeschaffung unterstützt, führte 2021 eine Umfrage zu personalisierten Stellenanzeigen durch. Dabei wurden 1.445 Teilnehmende im Zeitraum von Mitte März bis Ende April 2021 zu ihren Erfahrungen mit Stellenanzeigen und den Gestaltungen dieser befragt. Laut der Studie ist es den Befragten wichtig, dass eine Stellenanzeige auf ihre individuellen Bedürfnisse und Fähigkeiten zugeschnitten ist, da sie sich dadurch besser verstanden fühlen und sich eher mit der ausgeschriebenen Stelle identifizieren können. Eine personalisierte Stellenanzeige ermöglicht es ihnen, ihre Eignung für die Stelle besser einzuschätzen und ihre Entscheidung, sich zu bewerben, auf einer realistischeren Grundlage zu treffen. Somit kann eine personalisierte Stellenanzeige das Interesse potenzieller Arbeitskräfte wecken und die Wahrscheinlichkeit erhöhen, dass diese sich bewerben.

KI-basierte Tools

Eine weitere wichtige Entwicklung im Recruiting ist der Einsatz von KI-basierten Tools. Diese Tools helfen Unternehmen, Bewerbungen schneller zu verarbeiten und die Qualität der Bewerber*innen zu erhöhen. Ein Beispiel dafür sind Chatbots, die Fragen von Bewerbenden automatisch beantworten und sogar erste Bewerbungsgespräche führen können. Ein weiteres geeignetes KI-Tool sind Matching-Algorithmen, die in der Lage sind, die Anforderungen der Stellenausschreibung mit den erhaltenen Bewerbungen abzugleichen.

439404099 / Adobe Stock

Durch den Einsatz von KI können Unternehmen Zeit und Ressourcen sparen und sich auf die wichtigsten Aufgaben konzentrieren. Dadurch können Unternehmen geeignete Arbeitskräfte schneller und effizienter ansprechen und somit die Chancen auf eine erfolgreiche Einstellung erhöhen.

Social-Media-Kanäle

Ein weiterer Trend im Recruiting ist die Nutzung von Social-Media-Kanälen für das Ausmachen von Arbeitskräften. LinkedIn ist dabei das bekannteste soziale Netzwerk für berufliche Zwecke, aber auch andere Plattformen wie Facebook oder Twitter können genutzt werden. Unternehmen sollten Social-Media-Kanäle nutzen, um ihre Arbeitgebermarke zu stärken, potenzielle Kandidaten und Kandidatinnen zu finden und Informationen über Bewerbende zu sammeln.

Um neue Arbeitskräfte ausfindig zu machen, nutzen Unternehmen Mitarbeiterempfehlungsprogramme, um Mitarbeitende dazu zu ermutigen, offene Stellen in ihren sozialen Netzwerken zu teilen. So kann das Unternehmen auf qualifizierte Bewerber*innen aufmerksam gemacht werden und wird weiter verbreitet. Außerdem nehmen Unternehmen über soziale Medien an Karrieremessen und Netzwerkevents teil, um potenzielle Bewerbende zu erreichen und Beziehungen aufzubauen. Durch diese Maßnahmen können Unternehmen ihre Reichweite erhöhen und gezielter potenzielle Kandidaten und Kandidatinnen ansprechen.

Diversity und Inklusion

Ein weiterer wichtiger Trend im Recruiting ist die Bedeutung von Diversity und Inklusion. Unternehmen sollten sich bemühen, eine Vielfalt an Talenten zu gewinnen und zu fördern. Hierbei sollten auch Kandidaten und Kandidatinnen mit verschiedenen Hintergründen und Perspektiven berücksichtigt werden. Unternehmen, die sich auf Diversity und Inklusion konzentrieren, haben gezeigt, dass sie von einer höheren Produktivität und Kreativität ihrer Mitarbeitenden profitieren.

Diversity und Inklusion können dazu beitragen, das Wachstum eines Unternehmens zu fördern. Denn eine vielfältige Belegschaft trägt dazu bei, dass ein Unternehmen besser auf verschiedene Kundenbedürfnisse eingehen kann. Zusätzlich schafft Diversität innerhalb des Mitarbeiterstabs eine breitere Palette von Ideen und Perspektiven, die Unternehmen nutzen können, um ihre Geschäftsprozesse zu optimieren.

> Immer mehr Unternehmen setzen auf Diversity in ihrer Belegschaft. Eine Studie von McKinsey & Company von 2018 belegt, dass diese Unternehmen damit auch wirtschaftlich erfolgreicher sind. Die Studie wurde mit der Beteiligung von mehr als 1.000 Unternehmen aus 12 Ländern veröffentlicht und zeigt den Zusammenhang zwischen Diversity und Geschäftserfolg auf.

Mobile Recruiting

Ein weiterer wichtiger Trend im Recruiting ist das mobile Recruiting. Mobile Geräte wie Smartphones und Tablets sind heute allgegenwärtig und die meisten Bewerbenden nutzen diese Geräte, um Stellenanzeigen anzusehen und sich zu bewerben. Unternehmen sollten ihre Stellenanzeigen und Bewerbungsprozesse daher so gestalten, dass sie auf mobilen Geräten gut sichtbar und einfach zu bedienen sind.

Doch wie weit verbreitet ist mobiles Recruiting in Deutschland? Eine Studie von 2020 des Lehrstuhls für Wirtschaftsinformatik und Digitale Gesellschaft an der Universität Bamberg gibt Antworten. Die Studie untersuchte den Einsatz von mobilen Endgeräten im Recruiting-Prozess und zeigt, dass fast 90 % der Unternehmen in Deutschland mobile Geräte im Bewerbungsprozess einsetzen. Die Ergebnisse belegen außerdem, dass mobiles Recruiting den Bewerbungsprozess beschleunigt und erleichtert.

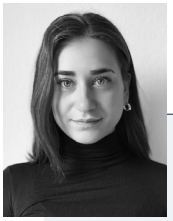
Mobile Recruiting kann dazu beitragen, dass Unternehmen mehr Bewerber*innen erreichen und ihre Chancen auf eine erfolgreiche Einstellung erhöhen.

Employer Branding

Ein weiterer wichtiger Trend im Recruiting ist das Employer Branding. Unternehmen sollten sich bemühen, eine starke Arbeitgebermarke aufzubauen und zu pflegen. Hierbei geht es darum, sich als attraktiver Arbeitgeber zu präsentieren und potenzielle Kandidaten und Kandidatinnen zu überzeugen, sich für eine Position zu bewerben. Employer Branding trägt maßgeblich dazu bei, dass Unternehmen die besten Talente gewinnen und halten können. Unternehmen sollten sich bemühen, ihre Arbeitgebermarke auf verschiedenen Kanälen zu präsentieren, einschließlich ihrer Website, Social-Media-Kanäle und Stellenanzeigen.

Fazit

Die heutige Recruiting-Landschaft ist anspruchsvoller als je zuvor, da Unternehmen sich mit den neuesten Trends vertraut machen müssen, um die besten Talente zu gewinnen und zu halten. Es gibt zahlreiche entscheidende Trends wie personalisierte Stellenanzeigen, KI-basierte Tools, Social-Media-Kanäle, Diversity und Inklusion, mobile Recruiting und Employer Branding, die Unternehmen nicht ignorieren sollten, um im Wettbewerb um die Top-Talente mithalten zu können. Indem Unternehmen diese Trends nutzen und ihre Recruiting-Strategien anpassen, können sie die besten Kandidaten und Kandidatinnen für ihr Unternehmen gewinnen und ihre Position auf dem Arbeitsmarkt stärken.



AUTORIN

Antonia Breitenfellner

Contentredakteurin in Berlin

Antonia Breitenfellner hat ihr Linguistik und Germanistik Studium erfolgreich abgeschlossen, ehe sie in die Marketingbranche wechselte und nun in Berlin als Contentredakteurin arbeitet. Nach Beendigung des Studiums und auf dem Weg in die Berufswelt stellte sie große Unterschiede in den Stellenanzeigen verschiedener Unternehmen fest und begann auf diesem Wege, sich genauer mit aktuellen Markttrends auf dem Jobmarkt auseinanderzusetzen.

Antonia Breitenfellner auf Linkedin

590510698/ Adobe Stock

Wie B2B-Surveys das wirtschaftliche Wachstum von Unternehmen beflügeln

von Alexander Friedrich

Unzufriedene Kunden und Kundinnen neigen dazu, Firmen miserable Zeugnisse auszustellen – ohne die betroffenen Unternehmen darüber in Kenntnis zu setzen. Diese wiegen sich häufig in trügerischer Sicherheit. Schließlich sind sie davon überzeugt, die Bedürfnisse ihrer Klienten und Klientinnen blind zu kennen. Ein leichtsinniger Irrglaube, der im schlimmsten Fall Kundenfluktuation nach sich zieht. Denn der Löwenanteil unglücklicher Kunden und Kundinnen verschafft seinem Unmut im eigenen Wirkungskreis Luft.

Verzichten Unternehmer auf eine kontinuierliche Optimierung ihres Waren- und Serviceangebots, riskieren sie, dass wertvolle Bestandskundschaft unbemerkt zu Mitbewerber*innen abwandern. Kundenzufriedenheitsumfragen beugen diesem Dilemma vor: Sie entledigen Firmen ihrer Blind Spots und strukturieren und komplettieren das Kundenmosaik. Eine kunstfertige Fragestellung offenbart dabei eine wahre Schatztruhe für Unternehmen.

> „Mittels Meinungs- und Marktforschung in den Dialog mit Kunden zu treten, führt oftmals zu nichts Geringerem als einem unternehmerischen Paradigmenwechsel – und genau den muss der Kunde im Ergebnis spüren“ – Steffen Köster, Geschäftsführer der niedersächsischen Marktforschungsagentur Umfrageheld

Wie und vor allem welche Fragen langfristig auf ein positives Betriebsergebnis einzahlen, zeigen die folgenden Einblicke.

Aufschlauen per Insiderwissen

Kunden-Surveys muten wie ein Realitätscheck an, in dem viel ökonomisches Potenzial steckt. Sie evaluieren die Treiber und Barrieren im Produkt- und Service-Portfolio eines Unternehmens und legen die Finger auf dessen Schmerzpunkte. Als zusätzlicher Kommunikationskanal zahlen fundierte Befragungen auf die Kundenbeziehung und -zentrierung ein. Firmen erhaschen einen Blick durch die Kundenbrille und generieren mit verhältnismäßig geringem Aufwand sogenannte Zero-Party-Daten – also Informationen aus erster Hand. Es lohnt sich, auf dieses Pferd zu setzen und folglich Zeit und Geld zu investieren. Im Ergebnis sorgt das für ein besseres Kundenverständnis und eine wachsende Empathie.

Kundenzufriedenheitsumfragen entledigen Unternehmen ihrer Blind Spots | Bildrechte: pexels.com

B2B-Erhebungen entzweien in diesem Zusammenhang den Begriff der Kundenzufriedenheit und betrachten seine Wortteile getrennt voneinander. „Bestandskunden stehen ohne Frage im Mittelpunkt des Geschehens, hier kommen operative sowie strategische Entscheidungen und Maßnahmen eines Unternehmens zum Tragen“, erklärt Steffen Köster. „Anhand des Wortes Zufriedenheit lässt sich verdeutlichen, wie vielfältig eine Kundenumfrage daherkommt. Ersetzen Unternehmensverantwortliche das höchste Qualitätsmerkmal durch Begrifflichkeiten wie Innovation, Produkt oder Preisbereitschaft, gewährt ihnen die Befragung einen ungeahnten, aber klärenden Deep Dive“, weiß der Experte für Marktforschung.

Gilt ein Unternehmen als innovativ? Treffen Produkte und Services den Nerv einer Zielgruppe? Besteht womöglich eine Betriebsblindheit? Solche Fragen eröffnen oftmals konkrete Handlungsempfehlungen, die im Umkehrschluss auch auf die Kundenzufriedenheit und das Umsatzwachstum einzahlen. Datenerhebungen geben zudem Aufschluss über und wertvolle Impulse zu folgenden Arbeitsbereichen:

- Iteratives Testing
- Verfeinerung von Marketingmaßnahmen
- Entdeckung und Erschließung von Marktlücken
- Produktentwicklung sowie Optimierung von Waren und Dienstleistungen

Daneben befeuern Kundenzufriedenheitsumfragen den Vorgang der Entscheidungsfindung, liefern sie doch kostbare Insights, die immensen Einfluss auf Prozesse wie Preis-, Sortimentsgestaltung und Unternehmenskommunikation nehmen.

Hegt der Kundenstamm selbst Interesse an einer Umfrageteilnahme, sichert dies den Erfolg einer B2B-Survey | Bildrechte: pexels.com

Die Kunst des Fragens

Mit Kunden und Kundinnen in den Dialog zu treten, erweist sich als leichte Übung. LinkedIn, Instagram, TikTok und Co. – Kommunikationskanäle gibt es mittlerweile wie Sand am Meer. Bei konkreten Fragestellungen besteht die Königsdisziplin für Unternehmen darin, Channels zu wählen, die sie ihrer Zielgruppe und damit möglichen Antworten näherbringen. Der Erfolg einer B2B-Survey als Instrument im Kundendialog steht und fällt mit der Qualität des Fragenkatalogs. Gezielte, wohlüberlegte Fragen, dem Kundenwunsch entsprechend, führen zum erwünschten Ergebnis. Schlecht aufgesetzte Fragebögen und Suggestivfragen bedeuten im schlimmsten Fall ein verzerrtes Abbild der Realität und ziehen fatale Fehlentscheidungen nach sich.

B2B-Erhebungen – eine Raketenwissenschaft? Keinesfalls! „Keep it simple“ – dieses Motto sollte über jeden Schritt von der Umfrageeinladung bis zur -auswertung schweben. Im Bestfall hegen Kunden und Kundinnen Eigeninteresse daran, an Befragungen mitzuwirken und ihre Meinung kundzutun. Damit es dazu kommt, müssen Fragebögen vorrangig Spaß machen. Auch der Grad der Komplexität darf nicht zu hoch sein. Geistige Bewandtnis, gewürzt mit einer guten Prise Bauchgefühl, lautet hier das Erfolgsrezept. Leads und Entscheidungsträgern, die sich das erste Mal mit der Befragungsthematik auseinandersetzen, empfehlen wir die Einhaltung des nachstehenden Fahrplans:

- **Überblick verschaffen**
  Markt- und Meinungsforschung, was steckt dahinter? Die Beantwortung dieser Frage markiert den Einstieg in die Thematik. Umfassende Recherchearbeiten und Website-Checks bei Statista und Survey Monkey gehören genauso dazu wie die Klärung des Begriffs Kundenzufriedenheit.

- **Pain Points evaluieren**
  In Zusammenarbeit mit einem festen Team oder einer Abteilung identifizieren Führungskräfte Schmerzpunkte aus Unternehmersicht. Diese bilden den vorläufigen Kern der späteren Kundenzufriedenheitsumfrage ab.

- **Zielgruppe definieren**
  Welchen Personenkreis soll die Datenerhebung ansprechen? Eine Clusterung der Kundengruppe nach Segmenten und Prioritäten ergibt häufig Sinn. A-, B- oder C-Kundenklasse – danach richtet sich maßgeblich die finale Gestaltung des Fragenkatalogs.

Kunden zu Fans machen

Wer B2B-Umfragen als Instrument zur Kundenkommunikation nutzt, sollte sich im Klaren darüber sein, dass es nicht ausreicht, das Tool lediglich ins unternehmerische Organigramm einzuflechten. Wortkosmetik löst konstruktive Kritik nicht in Luft auf, sondern ruft im Gegenteil Verärgerung auf Kundenseite auf den Plan.

Vielmehr heißt es, Ergebnisse der Meinungsforschung tatsächlich ins eigene Business zu integrieren und auf diesem Weg die Stammkundschaft an der Unternehmensentwicklung zu beteiligen. Ihre Anregungen und Wünsche fallen auf fruchtbaren Boden und rufen Veränderungen hervor. Um diese auf Nachhaltigkeit und Wirksamkeit zu überprüfen, raten wir zu einem Turnus von zwei Befragungen pro Jahr.

Wertbringende Ergebnisse abbilden und in konkrete Handlungsempfehlungen umwandeln – das ist die Kür. Überschaubare Charts, die Informationen wohldosieren, bringen Firmen ihre Schmerzpunkte verständlich und simpel aufbereitet bei. Was ergibt aus Service- und Dienstleistungsgesichtspunkten für den Kunden oder die Kundin wirklich Sinn? Befassen sich Unternehmen intensiv mit dem Feedback ihres Klientels, stärkt das die Kundenbindung, befeuert die Markenliebe und kurbelt den Umsatz an. Daneben können neuartige Begeisterungsmerkmale in Erscheinung treten, die Produktoptimierungs- sowie Entwicklungsprozesse beflügeln.

Auf Langstrecke erwachsen Kunden und Kundinnen von reinen Konsumenten zu Fans und agieren als potenzialträchtige Umsatzbeschleuniger. Denn wo Firmen Kunden-Surveys gekonnt nutzen, eröffnet sich die Chance auf ein maßgeschneidertes und organisch wachsendes Portfolio nach Kundenwunsch.

AUTOR

Alexander Friedrich
Business Development und Geschäftsführer Glückliche Kunden GmbH

Alexander Friedrich ist Experte für Kundenbindung. Der studierte Wirtschaftsingenieur bekleidet in seiner Vergangenheit diverse Lead-Positionen und greift auf tiefes Know-how im Umgang mit Kunden und Kundinnen zurück. Gemeinsam mit seiner Partnerin Karolina Friedrich entwickeln die beiden lösungsorientierte Trainingsprogramme, die den Fokus auf die Erhöhung der Kundenzufriedenheit sowie die Stärkung der Customer Relationship legen – Umsatzsteigerung inklusive.

Für den Beitrag stand er im Gespräch mit Steffen Köster, Geschäftsführer der Marktforschungsagentur Umfrageheld.

https://glueckliche-kunden.de/
Alexander Friedrich auf LinkedIn
hallo@glueckliche-kunden.de

TechDivision

Wir sind wieder Google Premium-Partner! Yeahh!

Unser Online-Marketing-Team gehört auch 2023 wieder zu den auserwählten 3 % Google Premium-Partnern in Deutschland.

Das wollen Sie testen? Sehr gerne!

Zur Feier des Tages gibt's nämlich einen kostenlosen SEA-Health-Check. Denn wir glauben, wir können aus Ihrem Google Anzeigen-Invest noch mehr herausholen. Und wir gehen dann mal feiern!

Zum Gratis SEA Check!

Ihr Kontakt zu uns:

www.techdivision.com
anfragen@techdivision.com

1935483316/ Adobe Stock

Feedback als Lösung gegen Personal-abwanderung

von Katerina Arsova

Wie konstruktives Feedback Vertrauen schafft und Mitarbeitende an das Unternehmen bindet

Aktuell macht vielen Unternehmen die Welle an Personalabwanderungen zu schaffen. Der Verlust von erfahrenen Teammitgliedern, die wertvolles Know-how mit sich nehmen, führt zu einem beträchtlichen finanziellen und zeitlichen Aufwand für Unternehmen – schließlich muss Ersatzpersonal gefunden und ausgebildet werden. Das gefährdet die Produktivität der Teams, die nun mögliche Engpässe füllen müssen. In Anbetracht des Fachkräftemangels ist es daher besonders wichtig, Mitarbeitende verstärkt an das Unternehmen zu binden.

Laut einer Studie des Instituts der deutschen Wirtschaft (IW) läuft die Situation Gefahr, sich noch weiter zuzuspitzen – bis zum Jahr 2030 könnten in Deutschland bis zu 3,3 Millionen Fachkräfte fehlen. Doch was verursacht Personalabwanderung und wie können Unternehmen präventiv handeln?

Eine oft übersehene Ursache für Personalabwanderung ist eine fehlende oder mangelhaft ausgereifte Feedbackkultur im Unternehmen. Denn bei richtiger Anwendung hat konstruktives Feedback das Potenzial, die Zufriedenheit von Teammitgliedern zu steigern und gleichzeitig Vertrauen zu schaffen – Vertrauen, das Mitarbeitende an ihre Teams und das Unternehmen bindet.

Zugehörigkeit und Loyalität als A&O für die Mitarbeiterbindung

Feedback verbindet Menschen sowohl auf professioneller als auch auf persönlicher Ebene. Es bewirkt, dass Mitarbeitende sich ernst genommen fühlen und wissen, dass ihr Entwicklungspotenzial anerkannt und gefördert wird. Zudem begünstigt Feedback eine verbesserte Kommunikation auf Teamebene: Es regt einen aktiven Austausch über Erfahrungen und Bedürfnisse an und lädt zur gegenseitigen Unterstützung ein. Das wiederum fördert die Bildung einer Gemeinschaft, in der sich Teammitglieder wohl und aufgehoben fühlen, was sich positiv auf ihre Arbeitsleistung und Produktivität auswirkt.

Hier gilt die Devise: Wertgeschätzte Mitarbeitende sind engagierte Teamplayer. Wenn Teammitglieder sich zudem mit dem Unternehmen sowie dessen Zielen und Werten identifizieren, bleiben sie der Organisation länger treu und sind dabei motivierter. Dadurch reduziert Feedback die Fluktuation und hilft Unternehmen, ihre Mitarbeitenden langfristig zufriedenzustellen und zu halten.

Feedback richtig kommunizieren – eine Checkliste für Unternehmen

Richtig Feedback geben will gelernt sein. Denn bei vielen Arbeitnehmenden löst der Gedanke an Feedback Ängste und Unsicherheiten aus. Häufig zu Unrecht! Konstruktives Feedback fördert das Wachstum der Teammitglieder, hebt ihre Leistungen hervor und gibt Impulse für Verbesserungen. Wichtig dabei: Feedback sollte stets sachlich, als inhaltliche Hilfestellung und Anregung zur persönlichen Entwicklung gegeben werden. Das Problem liegt bei destruktivem Feedback, das sich vorwiegend auf Negatives bezieht und oftmals weder situativ noch objektiv ist. Feedback als “Denkzettel” zu instrumentalisieren ist eine veraltete Herangehensweise und hat keinen Platz in einer modernen Feedbackkultur.

Zeitgemäß ist nur konstruktives Feedback, das neben Problemen auch Verbesserungspotenziale identifiziert und aufbauende, lösungsorientierte Kritik bietet. Es ist richtungsweisend und befähigt Mitarbeitende zu persönlicher und beruflicher Entwicklung. Solch wertvolles, umsetzbares Feedback fördert eine offene Kommunikation innerhalb des Unternehmens. Die dabei signalisierte Transparenz stärkt das Vertrauen und die Bindung der Mitarbeitenden.

Doch das Teilen von konstruktivem Feedback stellt für viele Führungskräfte eine Herausforderung dar. Wie, wann und wo sollte Feedback gegeben werden? Im Grunde gilt es, die folgenden Punkte zu beachten:

- Im ersten Schritt sollten die aktuelle Situation und die daraus resultierenden Konsequenzen erläutert werden. Ein Beispiel hierfür sind Teammitglieder, die häufig zu spät kommen und so ihr Team daran hindern, effektiv und ohne Verzögerungen zu arbeiten.

- Dabei ist es ebenso wichtig, klar zu kommunizieren und mittels Fragen den Austausch anzuregen.
- Konstruktives Feedback sollte in einer möglichst kleinen Runde geteilt werden – im Optimalfall unter vier Augen.
- Positives Feedback hingegen ist ein wirkungsvoller öffentlicher Ausdruck von Dankbarkeit und Wertschätzung.
- Dabei gilt es, auf das berüchtigte „Feedback-Sandwich" zu verzichten: Diese Methode, bei der eine Kritik zwischen zwei positiven Rückmeldungen geäußert wird, ist ein Grund, warum so viele Menschen Hemmungen vor Feedbackgesprächen haben und zynisch gegenüber Lob sind.

Werkzeug zur persönlichen und professionellen Weiterentwicklung

Mitarbeitende sind aus eigenem Antrieb sehr motiviert, sich weiterzuentwickeln. Sie erwarten individuelle Rückmeldungen und klar definierte Entwicklungsziele. Sprich, Mitarbeitende wünschen sich Feedback. Laut einer Umfrage von Gallup aus dem Jahr 2022 sind Arbeitnehmende fast viermal motivierter, starke Arbeit zu leisten, wenn sie kontinuierlich Feedback erhalten. Teammitglieder erwarten zudem zu Recht Anerkennung dafür, dass sie sich nicht nur fachlich, sondern auch persönlich weiterentwickeln wollen. Unternehmen sind nun am Zug, sie in dieser Entwicklung zu unterstützen – ansonsten laufen sie Gefahr, dass ihre Mitarbeitenden die einzige Chance auf Weiterentwicklung in einer Kündigung und den Neuanfang in einem anderen Betrieb sehen.

Zufriedene Teams als Status quo

Wie dieser Artikel zeigt, ist ein effektiver Weg der Personalabwanderung entgegenzuwirken das Implementieren einer ausgereiften Feedbackkultur. Zudem sollten innerhalb der Unternehmensstruktur Prozesse etabliert werden, die diese Kultur aufrechterhalten. Besonders wichtig ist, auf konstruktives Feedback zu setzen – und das nicht nur während der halb- bzw. vierteljährlichen Leistungsbeurteilungen, sondern kontinuierlich. Wenn Mitarbeitende das Gefühl haben, dass ihre Führungskräfte ihnen Vertrauen entgegenbringen und sich für ihre Förderung einsetzen, ist ein Jobwechsel nicht mehr die erste Option zur persönlichen und professionellen Weiterentwicklung. Dadurch spart das Unternehmen Zeit, Geld und Mühe, um die verlorenen Kompetenzen ehemaliger Mitarbeitender wiederzuerlangen – und ermöglicht eine gesteigerte Produktivität, Zufriedenheit und ein angenehmes Arbeitsklima.

AUTORIN

Katerina Arsova

Head of Talent Acquisition bei Leapsome

Katerina Arsova ist Head of Talent Acquisition bei der Personalentwicklungsplattform Leapsome, die mehr als 1500 Unternehmen (darunter Spotify, Unity und Monday.com) dabei hilft, die Weiterbildung, Produktivität und Bindung ihrer Mitarbeitenden zu fördern. Katerina wird von der Vision angetrieben, leistungsstarke, motivierte Teams aufzubauen. Vor ihrer Tätigkeit bei Leapsome verantwortete sie unter anderem Führungsrollen in der Talentakquise bei Flink, smava und Talent.io

https://de.leapsome.com/
Katerina Arsova bei LinkedIn

574691337 / Adobe Stock

Automatisierte und personalisierte Push-Nachrichten als Umsatz-Booster

von Olaf Brandt

Web Push und Tracking im E-Commerce

Der Corona-bedingte Boom im E-Commerce klingt langsam ab. Die neue Normalität hat für mehr Konkurrenz im Onlinehandel gesorgt, während die Finanzierung im Onlinebusiness heute deutlich schwieriger geworden ist. Daher steht Profitabilität jetzt im Fokus – insofern, dass Unternehmen den Kundenwert steigern und ausreichende Margen erzielen müssen. Hier kann Web Push als Alternative zu kostspieligen Ads den Traffic im Shop steigern und den Umsatz gezielt ankurbeln.

Doch wie lassen sich mehr Besucher*innen in den Shop locken und zum erneuten Kauf animieren? Der Schlüssel ist eine Kombination aus passgenauen Inhalten, Angeboten und Aktionen, die sich an individuellen Nutzerbedürfnissen orientieren. Dazu müssen sich Onlinehändler*innen das in ihrem Shop gezeigte Besucherverhalten zunutze machen, um die potenziellen Onlineshopper*innen mit relevanten Push-Nachrichten adressieren zu können.

Was ist Web Push?
Web-Push-Marketing ermöglicht die schnelle Übermittlung zielgerichteter Botschaften. Diese klickbaren Kurznachrichten heißen Push Notifications. Ähnlich wie bei WhatsApp oder SMS erscheinen diese Benachrichtigungen direkt – sogar auf dem Sperrbildschirm und bei Computern im Webbrowser. So können Shopbetreiber*innen schnell und in hoher Frequenz passgenaue, anlassbezogene Nachrichten an die Nutzer*innen senden. Grundlage für die Inhalte sind entweder Angaben der Nutzer*innen, welche zuvor – wie bei einem klassischen Newsletter – Themen (z. B. Erneuerbare Energien), Produktsegmente (z.B. Ökostrom) oder Regionen (z.B. Norddeutschland) über eine Checkbox ausgewählt haben. Oder die Nachrichten werden anhand des Nutzerverhaltens auf der Website personalisiert und automatisiert versendet.

Je nachdem, welches Verhalten eine interessierte Person zeigt, fungiert dies als Trigger (Auslöser) für den automatischen Versand einer passenden Push-Nachricht. Somit lassen sich laufende Aktionen mit kleinen Botschaften pushen oder individuell passende Inhalte gezielt an Nutzer*innen übermitteln – aber eben nicht im Broadcasting-Style, sondern personalisiert und automatisiert. Das fördert nicht nur den erfolgreichen Abschluss von Shoppingprozessen, sondern auch das Cross- und Upselling.

Getracktes Nutzerverhalten für die personalisierte Ansprache nutzen

Um das Verhalten von Shopbesuchern auf individuelle Nutzer*innen herunterzubrechen und diese dann mit dazu passenden Botschaften anzusprechen, haben E-Commerce-Unternehmen grundsätzlich zwei Möglichkeiten:

Push Notifications erscheinen direkt im Webbrowser oder auf dem mobilen Display – sogar auf dem Sperrbildschirm. (Quelle: signalize.com)

1. Sie bauen sich aus Trackingdaten und Kaufhistorien eine umfassende Customer Data Platform (CDP) auf und koppeln die darin enthaltenen Daten mit einer Web-Push-Lösung. Das verursacht großen Aufwand wie auch Kosten und ist – insbesondere für kleinere Onlinehändler*innen – kaum zu bewerkstelligen.

2. Sie setzen auf ein statisches Triggering, welches jeden Trigger einzeln definiert und in die Website und Push-Lösung einbaut. Allerdings besteht auch hier ein nicht unerheblicher Implementierungsaufwand, weil es jeden neuen Trigger erst zu integrieren gilt. Den Auslöser nachträglich beziehungsweise rückwirkend einzustellen, ist nicht möglich. Onlinehändler*innen müssen also immer vorher wissen, auf Basis welcher Trigger sie ihre Shopbesucher*innen ansprechen möchten.

Eine elegantere, alternative Lösung bietet hier ein in die Web-Push-Lösung integriertes Tracking. Damit stehen – ohne die Vorabimplementierung von Triggern – sämtliche Verhaltensdaten des Shopbesuchers automatisch zur Verfügung und ließen sich auf Wunsch sogar an eine CDP an-

koppeln. Hat sich beispielsweise ein Besucher oder eine Besucherin drei oder mehr Kühlschränke im Onlineshop angesehen, aber kein Produkt in den Wagen gelegt, kann dieses Verhalten direkt als Trigger für bestimmte Push-Nachrichten dienen. Weiter differenzieren ließe sich dies zum Beispiel nach angesehenen Marken oder danach, ob zugehörige Videos und Einkaufsratgeber angeschaut wurden. Statt bei jeder Änderung oder Verfeinerung der Trigger die Implementierung im Shop anpassen zu müssen, stehen beim integrierten Tracking ohnehin alle denkbaren Verhaltensdaten zur Verfügung. Aus diesen lässt sich dann ein geeigneter Trigger flexibel einstellen.

Zehn spannende Trigger für umsatzfördernde Push-Nachrichten

In der nachfolgenden „Triggerbatterie" finden sich etliche Anlässe, die als Hidden Champions vielfach ungenutztes Potenzial haben:

1. Ein stehen gelassener Warenkorb sowie die enthaltenen Produkte
2. Besuchte Produktkategorien
3. Eingegebene Suchbegriffe im Shopfinder
4. Ausstieg bei der internen Suche sowie abgebrochene Produktrecherchen
5. Abbruch im Check-out-Prozess
6. Lange Zeitspanne seit dem letzten Websitebesuch
7. Nutzung bestimmter Funktionen im Onlineshop (z. B. Größenrechner)
8. Zuletzt gekaufte Produkte
9. Angeklickte interne Teaser bzw. Promotions
10. Absprungverhalten (Bouncing)

Für das hohe Maß an Personalisierung und damit eine noch größere Umsatzchance lassen sich Trigger auch beliebig miteinander kombinieren: So können Onlinehändler*innen beispielsweise Kunden, die von einem Artikel unterschiedliche Größen in den Warenkorb legten, aber beim Punkt „Versand- und Retourkosten" im Check-out-Prozess abbrechen, einen Gutschein-Code für den kostenfreien Versand und Rückversand anbieten oder generell die Aktion „Bestellen, anprobieren, kostenfrei zurücksenden" via Push-Nachricht promoten.

Personalisierung – auf Knopfdruck

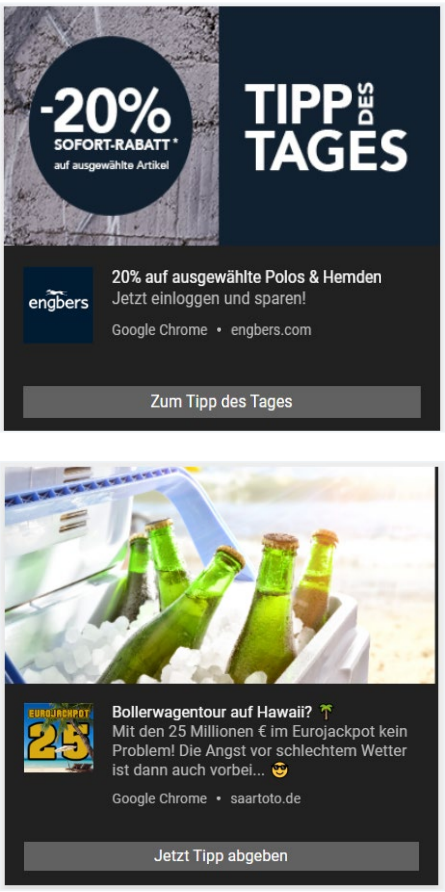
Onlinehändler*innen sollten es unbedingt ausnutzen, dass sich beliebige Trigger jederzeit aufgreifen lassen. Natürlich funktioniert auch das statische Triggering mit nur vorab eingebauten Triggern, schränkt aber die Möglichkeiten des Web-Push-Marketings immens ein. Statt sich also im Vorfeld umständlich mit den passenden Triggern auseinandersetzen zu müssen, haben Shopbetreiber*innen die Chance, sich von den Verhaltensdaten inspirieren zu lassen, zu schauen, welche Trigger sich anbieten und dadurch noch näher an ihrer Zielgruppe zu sein. Mit dem richtigen Web-Push-Tool können sie Trigger spontan entdecken und direkt nutzen sowie auch auf historischen Daten aufbauen.

Wenn etwa das Interesse an einer bestimmten Produktkategorie immer wieder saisonal ansteigt, kann man bereits hier eine entsprechende Push-Kampagne vorbereiten. Aber auch eine eben erst abgebrochene Produktsuche kann direkt als Trigger fungieren, damit die Shopbesucher*innen per Push-Nachricht einen Hinweis erhalten, dass es noch vergleichbare Produkte oder Rabattaktionen gibt: „Nicht das Passende gefunden? Hier findest du ähnliche Artikel!" Oder: „Noch unsicher? Bestelle jetzt und spare die Versand- und Retourenkosten!" Ist einmal ein passender Trigger entdeckt, lassen sich die Push Notifications vorbereiten. Bei der Gestaltung der Kurznachrichten sind der Kreativität der Onlinehändler*innen keine Grenzen gesetzt. Wenn jetzt wieder ein

Shopbesucher seine Suche abbricht, bekommt er die gleiche Nachricht – gegebenenfalls mit den dann individuell passenden Links zu ähnlichen Produkten.

Noch mehr Möglichkeiten durch Automatisierung

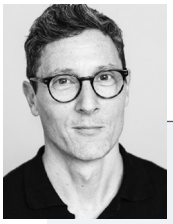
Noch mehr Potenziale können Shopbetreiber*innen durch die Verknüpfung mit ERP- oder Order-Management-Systemen erreichen: Auslöser für Push-Nachrichten sind dann nicht die Aktivitäten der Nutzer*innen, sondern Veränderungen im Warenbestand – wie etwa neu aufgenommene oder wieder verfügbare Artikel oder auch Preisreduzierungen. Kombiniert mit Informationen darüber, für welche Nutzer*innen diese News relevant sind, lässt sich die Kommunikation mit den Shopbesuchern noch weiter personalisieren und automatisieren. Das bedeutet für Shopbetreiber*innen nicht nur mehr Umsatzchancen, sondern auch einen erheblichen Effizienzgewinn.



Personalisierte Push Notifications steigern die Klick- und Kaufwahrscheinlichkeit. (Quelle: signalize.com)

Fazit: Push-Service als Umsatz-Booster 2023

Web Push gehört als Kanal für viele E-Commerce-Unternehmen bereits dazu. Sein Potenzial bleibt allerdings meist unausgeschöpft. Dabei schlummern hier wertvolle Umsatzchancen, die sich mit einer trackingbasierten Automatisierung und Personalisierung des Web-Push-Kanals im Handumdrehen nutzen lassen. Im Vergleich zu vielen anderen Marketinginstrumenten und -formaten sind Push Notifications zwar nur kleine Botschaften, aber durch ein Web-Push-Tool mit integriertem Tracking lassen sich hochgradig personalisierte Nachrichten zielsicher an die richtigen Shopbesucher*innen ausspielen. So bekommen Onlinehändler*innen ihre Kundschaft nicht nur erneut in den Shop und vom Kauf überzeugt, sondern helfen den Onlineshoppern bei ihren Herausforderungen und verbessern das Einkaufserlebnis nachhaltig.



AUTOR

Olaf Brandt
Geschäftsführer etracker GmbH

Olaf Brandt ist Geschäftsführer der etracker GmbH, dem Experten für datenschutzkonformes Tracking. Nachdem der Diplom-Kaufmann in verschiedenen Softwareunternehmen beschäftigt war, kam Brandt 2008 zu etracker, wo er zunächst im Business Development tätig und später für die Produktentwicklung der Web Push-Lösung Signalize verantwortlich war. Signalize basiert im Kern auf der etracker Tracking-Technologie, wodurch Automatisierungen und Segmentierungen per Plug-and-Play zur Verfügung stehen. Für den Versand von Push-Nachrichten via Signalize bedarf es immer der Einwilligung des Nutzers, während die Messung mit etracker Analytics im Standard keiner Einwilligung bedarf.

https://www.etracker.com/
https://signalize.com/
Olaf Brandt auf LinkedIn

eSTRATEGY

Sie wissen genau, was Sie da tun?

Prima!
Dann teilen Sie Ihr Fachwissen doch mit uns.

Wir suchen Sie! Als Gastautor*in für das eStrategy-Magazin schreiben Sie über spannende Themen wie: E-Commerce, Digital Business, Online-Marketing, Projektmanagement, Mobile oder Webentwicklung. Wir freuen uns auf Sie!

Jetzt Gastautor*in werden!

www.estrategy-magazin.de

379358186 / Adobe Stock

Produktdaten-management, PXM & Co.

von eStrategy-Redaktion

Interview mit Benoit Jacquemont, Co-Founder und CTO bei Akeneo

Um Erfolg in der digitalen Welt zu haben, spielen bestmögliche Produktdaten und die Bereitstellung dieser Daten für unterschiedlichste Kanäle eine zentrale Rolle. Das Ganze hat inzwischen auch einen Fachbegriff – Product Experience Management (PXM). Der PIM Anbieter Akeneo hat sich bereits sehr früh diesem Thema verschrieben.

Wir haben mit dem Mitgründer und CTO von Akeneo, Benoit Jacquemont, über Produktdatenmanagement, PXM als Basis für herausragende Customer Experience und einige Neuigkeiten bei Akeneo gesprochen.

Hallo Benoit, bitte stell Dich kurz vor.

Hallo, ich bin Benoit. Ich bin Mitgründer und CTO von Akeneo. Die meiste Zeit verbringe ich mit unserem Produktteam hier bei Akeneo, aber ich diskutiere auch gerne mit Interessenten und Kunden. Meiner Meinung nach ist Technologie dazu da, dem Kunden zu mehr Geschäft/Erfolg zu verhelfen.

Wie seid Ihr auf die Idee gekommen, Akeneo zu gründen? Was waren die Beweggründe dafür?

Mit Fred de Gombert und Nicolas Dupont arbeitete ich bei einem großen französischen Systemintegrator. Um 2008 herum begannen wir, mehr und mehr E-Commerce für ziemlich große Marken und Einzelhändler zu erstellen. Aber unabhängig von der Größe der Kunden und ihrer Reife im digitalen Handel standen wir immer vor demselben Problem: Die Verwaltung von Produktinformationen war für sie mehrheitlich ein großes Problem.

Also haben wir versucht, eine Lösung für dieses Problem zu finden. Wir sahen uns um und versuchten eine Software zu finden, die wir zur Verwaltung der Produktinformationen integrieren konnten. Aber nichts, was wir fanden, entsprach wirklich den Anforderungen unserer Kunden. An diesem Punkt fragte uns Fred eines Tages: „Hey Leute, warum bauen wir nicht selbst eine entsprechende Software?“. Das war die Geburtsstunde von Akeneo.

Was war Euer Ziel, als Ihr das Unternehmen gegründet habt? Hat sich dieses Ziel mit der Zeit verändert?

Das ursprüngliche Ziel war es, die Probleme des Produktinformationsmanagements zu lösen: Nichts war zentralisiert, die Qualität der Daten war sehr schlecht und manchmal existierten sie einfach noch gar nicht. Das war die allererste Ebene der Probleme, die wir angehen wollten. Dann wuchsen wir mit unseren Kunden und erkannten, sobald wir unseren Kunden geholfen hatten, diese grundlegenden Bedürfnisse zu lösen, konnten sie sich darauf konzentrieren, ihren eigenen Kunden durch hochwertige Produktinformationen einen echten Mehrwert zu bieten.

Wir stiegen in der Maslowschen Pyramide der Produktinformation auf und wir begannen, uns darauf zu konzentrieren, was die Endkunden durch ihren Kontakt mit Produktinformation erleben. Daraus wurde das Product Experience Management – auch bekannt als PXM. Unsere Aufgabe bestand und besteht darin, unseren Kunden die Werkzeuge und Praktiken zur Verfügung zu stellen, damit sie eine bestmögliche Produkterfahrung bereitstellen können.

Akeneo feiert dieses Jahr sein zehnjähriges Bestehen. Was waren die größten Highlights für Dich in dieser Zeit?

Ganz klar die Menschen im Allgemeinen! Unsere Partner, die uns vertraut haben und mit uns die Zukunft von PXM aufbauen. Unsere Kunden, die auf uns gesetzt haben, als wir gerade anfingen und die, die uns heute herausfordern. Die Leute, die vor 10 Jahren zu Akeneo kamen, als wir noch nicht einmal ein richtiges Büro hatten. Und die, die jetzt zu Akeneo kommen und bereit sind, die nächste Stufe der Digitalisierung zu erreichen. Es gibt so viele Dinge, die man von all diesen Menschen lernen kann!

Was waren die größten Überraschungen und Lektionen oder Rückschläge auf Deiner bisherigen Akeneo-Reise?

Diese 10 Jahre fühlen sich wirklich seltsam an – sowohl extrem schnell als auch gleichzeitig außerordentlich langsam. So viele Dinge wurden angestoßen und erreicht. Zur gleichen Zeit gibt es Dinge in unserer ursprünglichen Vision, die wir noch nicht erreicht haben. Ich würde sagen, es ist das Waldsyndrom: Man kann das Ausmaß des Waldes nur sehen, wenn man auf die Spitze eines Baumes klettert. Aber Du wirst immer einen höheren Baum am Horizont sehen, der dir einen deutlich besseren Blick auf den Wald ermöglicht. Du gehst also zu diesem höheren Baum. Du kletterst hinauf. Siehst, dass der Wald noch größer ist als das, was Du vorher gesehen hast und höchstwahrscheinlich siehst Du einen anderen, noch höheren Baum in der Ferne …

Das ist mein größtes Learning: Es gibt immer mehr zu lernen und zu tun!

Der Markt für PIM-Systeme hat sich in den vergangenen Jahren sehr dynamisch entwickelt und es gibt inzwischen eine große Anzahl verschiedener Anbieter. Warum sollte ein Kunde Akeneo als Softwarelösung für sein Produktinformationsmanagement wählen? Wo siehst Du den USP von Akeneo?

Die klare, einfache Benutzeroberfläche und Bedienung war und ist immer noch eines der großen Unterscheidungsmerkmale für Akeneo. Ein weiteres Unterscheidungsmerkmal ist für mich die Fähigkeit, sehr große Kataloge mit Millionen von Produkten zu handhaben, wobei das Produktdatenmodell absolut flexibel bleibt.

Akeneo war eines der ersten Unternehmen, das den Begriff Product Experience Management (PXM) verwendete. Was genau verbirgt sich dahinter und warum ist es Deiner Meinung nach wichtig, dass sich Unternehmen damit beschäftigen?

Ich habe diesen Punkt vorhin schon ein wenig angeschnitten. Der Grundgedanke von PXM ist, dass unsere Nutzer bestmögliche Produkterfahrungen für ihre eigenen Kunden schaffen können. Dank der richtigen Tools können sie den Produktivitätsgewinn nicht nur nutzen, um mehr Zeit mit der Entwicklung dieser Erfahrungen zu verbringen, sondern sie können diese auch an einem zentralen Ort verwalten, der alle ihre Kanäle bedient. Und das ist für Unternehmen besonders wichtig, weil sich die Kontaktpunkte zwischen potenziellen Kunden und Produkten vervielfachen: E-Commerce-Website, Ladengeschäft, TikTok-Video, Marktplätze usw. …

Unsere Nutzer können also nicht die volle Kontrolle über die Art und Weise, wie dieser Kontakt zustande kommt, übernehmen, aber sie haben die Kontrolle über die Produkterfahrung, die sich aus diesen verschiedenen Kontaktpunkten ergibt. Das ist der Punkt, an dem das Product Experience Management seine ganze Bedeutung erhält.

Lass uns einen Blick in die Zukunft werfen: Was ist Dein Ziel und Deine Vision mit Akeneo kurzfristig in den nächsten 12 Monaten und mittelfristig in den nächsten 2–3 Jahren?

Unsere kurz- und mittelfristigen Ziele drehen sich alle um unsere Product Cloud Vision. In den nächsten 12 Monaten wird eine große Komponente dieser Vision, unsere Product Data Platform (PIM), eine noch viel größere Rolle in unserem Ökosystem spielen – primär durch die Erweiterung über unterschiedliche Apps. Und in den nächsten 2-3 Jahren werden wir diese Vision der Product Cloud weiter ausbauen und ausbilden.

Akeneo hat schon seit einiger Zeit eine strategische Partnerschaft mit Adobe. Was hat es damit auf sich und welche Ziele verfolgt Ihr mit dieser Partnerschaft?

Akeneo ist der bevorzugte PIM-Partner von Adobe. Und in der Tat, Adobe Commerce ist ein wichtiger Akteur in der Welt der E-Commerce-Plattformen. Diese Partnerschaft ermöglicht es uns, als PIM für Adobe Commerce Kunden empfohlen und auch relativ einfach angebunden zu werden.

Akeneo hat letztes Jahr die Akeneo Product Cloud eingeführt. Ist dies eine neue Version Eurer PIM-Lösung oder was genau verbirgt sich dahinter? Was ist der Unterschied zwischen PIM und Product Cloud?

PIM ist eine wichtige Komponente der Product Cloud. Die Product Cloud ist ein zentraler Ort, an dem alle Produktinformationen gespeichert, gepflegt und über verschiedenste Konnektoren an die unterschiedlichen Kanäle ausgespielt werden können. Wenn wir im Fall der Product Cloud von Produktinformationen sprechen, dann ist das weiter gefasst als das, was wir normalerweise in einem PIM finden. In der Product Cloud finden wir unter anderem Bestandsinformationen, Preise, Nutzerbewertungen, aber auch Informationen über die Verkaufsleistung eines Produktes. Das Konzept der Product Cloud besteht darin, Akeneo Usern eine 360°-Sicht auf Produktinformationen zu geben.

Ende Februar 2023 wurde Akeneo von Ventana Research zum „Value Index Leader“ ernannt. Was bedeutet das genau und warum ist diese Auszeichnung wichtig bei der Auswahl eines PIM-Systems?

Als Spezialist für Lösungen zur Verwaltung von Produktinformationen und Produkterfahrungen ist es natürlich wichtig, von Ventana anerkannt zu werden. Für mich ist hier aber besonders die Auszeichnung in der Kategorie „Validierung“ der Ventana-Studie wichtig, in der Akeneo als führend angesehen wird. Diese Kategorie steht für die Fähigkeit des Anbieters, den Kunden während seiner gesamten PXM Journey zu unterstützen. Und das ist sicherlich eines der Unterscheidungsmerkmale von Akeneo als ein Unternehmen, das die Werkzeuge, Prozesse und das Wissen bereitstellt, das unsere Kunden nutzen, um ihre PXM-Praxis zu initiieren und auszubauen.

Auf der jüngsten Unlock-Konferenz in Paris habt Ihr eine Reihe von Innovationen und neuen Funktionen vorgestellt. Bitte gib uns einen kurzen Einblick in das, was bei Akeneo neu ist und worauf sich die Kunden in Zukunft freuen können.

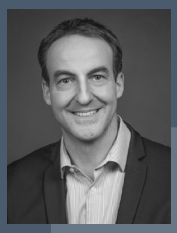
Wir arbeiten an vielen verschiedenen und sehr spannenden Themen! Es gibt eine Aufzeichnung einer entsprechenden Session auf der Konferenz. Hier würde ich aber auf jeden Fall das neue Akeneo Activation for Retail Feature hervorheben. Damit können wir unsere Kunden auf ihrer Product Experience Management Reise auf einem neuen Level begleiten.

Was würdest Du Unternehmen raten, die sich mit dem Thema Produktdatenmanagement beschäftigen und auf der Suche nach einer geeigneten Lösung und einem entsprechenden Dienstleister sind? Wie sollte man hier aus Deiner Sicht idealerweise vorgehen?

Wir haben ein Assessment entwickelt, das ein ausgezeichneter Ansatzpunkt sein kann: https://www.akeneo.com/pxm-maturity-path/

Je nachdem, wo das Unternehmen steht, sollte die Strategie zur Lösung der Probleme im Kontext des Produktdatenmanagements unterschiedlich betrachtet werden. Aus dieser Strategie kann das Unternehmen dann ableiten, wie die passende Lösung aussehen soll und aus dieser Lösung dann den richtigen Dienstleister mit der entsprechenden Erfahrung ableiten.

Vielen Dank für das Gespräch, Benoit!



INTERVIEWPARTNER

Benoit Jacquemont

Co-Founder und CTO bei Akeneo

Bevor er Akeneo gründete, war Benoit Jacquemont CTO bei Smile, dem größten Open-Source-Systemintegrator in Europa. Er ist Experte für komplexe Webanwendungen und hat in den vergangenen 5 Jahren ein Team von mehr als 450 Open-Source-Entwicklern geleitet und einige der größten europäischen Websites gelauncht. In seiner Freizeit gilt seine Leidenschaft dem Bauen und Fliegen von Modellflugzeugen, einige davon hängen allerdings noch in den Bäumen … ;-).

https://www.akeneo.com/de/
Benoit Jacquemont auf LinkedIn

100301160 / Adobe Stock

Erfolgschancen im B2B-Marketing erkennen

von Hartmut König

Nah an der eigenen Kundschaft sein, ihr Anliegen kennen und mit nahtlosen Erlebnissen über alle Kanäle hinweg zu punkten, ist längst nicht mehr nur Sache des B2C. Auch im B2B-Bereich wünschen sich Einkäufer*innen zunehmend die gleichen Erlebnisse, die sie privat gewöhnt sind. Um das zu erreichen, muss als Herzstück einer herausragenden Customer Experience die emotionale Verbindung zwischen Mensch und Marke im Vordergrund stehen. Marketing-Automatisierung kann dabei unterstützen, personalisierte datengetriebene Kundenkommunikation im B2B-Bereich voranzutreiben.

Die Anforderungen an erfolgreiches B2B-Marketing haben sich in den letzten Jahren stark gewandelt – Käufer*innen sowie Kunden und Kundinnen erwarten heute digitale Interaktionen. Laut der aktuellen Studie „Status der Marketing Automatisierung" gaben 97 % der befragten B2B-Entscheider*innen an, die Bereitstellung großartiger Käufer-/Kundenerlebnisse als eines der wesentlichen Ziele zu betrachten. Diese Entwicklung unterstreicht nur umso deutlicher die wachsende strategische Bedeutung des Marketing und die Bereitstellung hervorragender Erlebnisse. In einer Umgebung, in der Vertrauen als Währung den Unternehmenserfolg sichert, ist jede einzelne Kundenbeziehung von unschätzbarem Wert. Einige führende Marketingorganisationen haben sich mit ihren Best Practices als Vorreiter identifiziert. Ihre ausgereiften Leistungen lassen sich dabei in fünf Bereiche einteilen, die alle auf Daten und Technologien basieren.

1. Zweckmäßige Strategie und Taktik

Kundenerwartungen, Marketingstrategien und auch Marketing-Tools entwickeln sich heute schneller denn je. Die Unbeständigkeit macht eine Priorisierung häufig zum Ratespiel. Vorreiter setzen deshalb auf eine Perspektive von außen nach innen. Es ist wichtig, zuerst die Marktchancen zu erkennen, Ziel-Accounts zu definieren und einflussreiche Käuferprofile zu erstellen, um mit einer personalisierten Customer Journey zum Zielprodukt zu führen. Notwendig ist eine Balance zwischen Personen- und Account-basierten Strategien, denn ein zielgerichtetes Targeting erlaubt eine präzisere Interaktion mit Kunden und Kundinnen.

2. Abstimmung zwischen Vertrieb und Marketing

Ganze 98 % der Vorreiter rechnen damit, dass die enge Abstimmung von Marketing und Vertrieb jetzt und auch zukünftig eine essenzielle Notwendigkeit bleibt. Eine enge Partnerschaft beider Bereiche war im B2B schon immer wichtig, aber Faktoren wie die Pandemie haben digitale Verkaufsmethoden stark vorangetrieben. Der digitale Handel erfordert größte Sorgfalt. Interaktionen müssen gut koordiniert und markenkonform ablaufen, gleichzeitig muss die Privatsphäre der Kunden und Kundinnen gewährleistet werden. Auch Marketing Operations werden künftig

4151165601 / Adobe Stock

noch wichtiger – davon sind 100 % der Vorreiter überzeugt. Bei Marketing und Vertrieb steht heute nicht nur der Wert neuer Kundschaft im Mittelpunkt, vielmehr geht es darum, erfolgreiche langlebige Geschäftsmodelle zu integrieren und Interessenten langfristig an sich zu binden. Über eine Marketing-Automatisierungsplattform lassen sich alle digitalen Marketingaktivitäten und der hierfür greifbare Datenverkehr verwalten. So lässt sich unter anderem der Prozess der Leadgenerierung optimieren und anhand der nachvollziehbaren Customer Journeys innerhalb der Marketingabteilung teamübergreifende personalisierte Kampagnen gestalten. Auch die Vertriebsteams können Daten via Transfer so für koordinierte Journeys nutzen.

3. Personalisierung ist Key

B2B-Käufer*innen und Kundinnen sowie Kunden erwarten die gleichen personalisierten Erlebnisse im Arbeitsleben, die sie privat im Onlinehandel erfahren. Konsequente Personalisierung, wie sie Vorreiter anbieten, fördert laut einer Studie von McKinsey von November 2021 „die Performance und die Kundenergebnisse“. Ganze 40 % des Unternehmenswachstums lassen sich auf die Personalisierung zurückführen. Dazu gehören zentralisierte Kundendaten, Content-Erstellung, Omnichannel- Customer-Journeys und Messungen. Auch hier ist vieles eine Frage passender technologischer Lösungen, die die Komplexität von B2B bewältigen können – etwa Verknüpfungen zwischen Menschen und Accounts oder phasenspezifischer Content. Besonders die Präsentation personalisierter Inhalte sowie die Beschaffung der hierfür benötigten Kundendaten gehören mit jeweils 73 % zu den größten Herausforderungen, denen Vorreiter mit Technologie begegnen.

4. Einwandfreie Orchestrierung

Orchestrierte Interaktionen sind der Schlüssel zu einer nahtlosen Kundenkommunikation. Dafür müssen B2B-Vermarkter*innen die Kundschaft auf ihren bevorzugten Kanälen abholen. Customer Journeys sind heute dynamisch, Cross-Channel-Interaktionen die Regel. Ein mittlerweile besonders beliebter Interaktionskanal ist der Chat – hier können Kunden und Kundinnen die Kommunikation frei nach eigenen Bedingungen gestalten und ein Supportservice kann auf das gewünschte Anliegen reagieren. Ist ein Problem schnell gelöst, fördert das wiederum die Zufriedenheit. 90 % der befragten B2B-Entscheider*innen möchten in diesem Jahr einen Website-Chat implementieren oder diesen verbessern. Je mehr Kanäle es zu verwalten gibt, desto höher ist auch der Orchestrierungsbedarf – hier können moderne Automatisierungstechnologien und KI manuelle kleinteilige Aufgaben übernehmen. Ob Lead- oder Account-basiertes Marketing, für eine erfolgreiche Orchestrierung setzen Vorreiter auf wesentliche Funktionen wie Scoring, Phasen-Tracking, Routing sowie Zielgruppen- und Aktivitäts-Trigger, um schnell auf neue Veränderungen im Kundeninteresse reagieren zu können.

5. Marketingwirkung messen

Erst mit der Attribution lässt sich sicher definieren, welche Kampagnen, Kanäle und Inhalte eine businessrelevante Wirkung erzielen. Sie gibt Aufschluss darüber, welche Strategie in welcher Phase der Interaktion für welche Kundengruppe am besten funktioniert hat. Im B2B-Bereich sind diese Messungen häufig nicht ganz einfach durchzuführen, da die Zahl der Marketing- und Vertriebs-Touchpoints nicht selten in die Hunderte gehen. Eine sinnvolle Performancemessung kann mit einem kampagnenbasierten Multi-Touch Attribution-Report erzielt werden. Einige Marketing-Automatisierungsplattformen bieten hier einen leichten Einstieg.

Datenqualität und Technologie für bessere Erlebnisse

Kundendaten sind die Grundlage für eine hervorragende Planung, Interaktion und Messung. Zu den wichtigsten Marketing-Automatisierungsfunktionen von B2B-Entscheider*innen gehört neben dem Account-basierten Marketing und der Content-Personalisierung vor allem die Unterstützung durch KI. Die Anforderungen, komplexe Kundenwünsche erfolgreich abzudecken, sind hoch, aber mit einem starken MarTech Stack, dem Fokus auf Personalisierung und der richtigen Messung sind Unternehmen gut aufgestellt, um zukünftig den Erfolg zu sichern.

AUTOR

Hartmut König

CTO Central Europe bei Adobe

Hartmut König unterstützt Unternehmen bei ihrer digitalen Transformation und der Bereitstellung herausragender Kundenerlebnisse. Als Schlüssel zum Erfolg dieser Strategie sieht er die Verfügbarkeit großer Datenmengen, die es ermöglichen, relevante Inhalte bereitzustellen und durch Künstliche Intelligenz zu aktivieren.

Seine Karriere bei Adobe begann Hartmut König bereits 2004 und ist heute CTO Central Europe. Neben seiner langjährigen Erfahrung in der Beratung und im Projektmanagement hat Hartmut König den eigenen digitalen Transformationsprozess von Adobe seit 2008 aktiv begleitet.

In seiner Zeit bei Adobe bekleidete Hartmut König diverse leitende Positionen und verantwortete Projekte in den Bereichen Consulting, Pre-Sales Solutions Consulting und als Director des Specialist Sales Teams. Weitere wichtige Stationen seiner Karriere waren m+s Elektronik AG, Objective Software und SDL.

https://business.adobe.com/de/
Hartmut König auf LinkedIn

Literatur & Links

Alle genannten Werte beziehen sich auf die Ergebnisse der Adobe-Studie „Status der Marketing-Automatisierung“, die unter 600 Befragten Teilnehmer*innen, darunter Führungskräfte sowie Nutzer*innen von Marketing-Automatisierung aus Nordamerika durchgeführt wurde. Im Fokus stehen dabei besonders die befragten Vorreiter – Personen dieses Segments wiesen die beste Performance in den wichtigsten Marketing-Zielen auf. Die restlichen Teilnehmer*innen unterteilen sich in obere Mehrheit, untere Mehrheit sowie Nachzügler.

Adobe

Digitales Fundament.

Adobe – der richtige Partner für euer digitales Fundament.

Wir helfen euch bei der Umsetzung einer kundenorientierten digitalen Transformation auf einem Fundament aus Inhalten, Daten und KI, damit ihr individuelle und skalierbare Customer Experiences kreieren könnt.

Findet heraus, warum ein digitales Fundament so wichtig ist.

Mehr erfahren

© 2022 Adobe. Adobe und das Adobe-Logo sind eingetragene Marken oder Marken von Adobe in den Vereinigten Staaten und/oder anderen Ländern.
Alle anderen Marken sind Eigentum der jeweiligen Inhaber

310449548 / Adobe Stock

Verkaufspsychologie in Videos

von Katharina Schneider

4 Techniken für höhere Konversion

Die wirksame Anwendung von Werbepsychologie ist eine wertvolle Unterstützung zur Optimierung Ihres Marketings sowie zur Gestaltung konversionsstarker Videos. Bei der Erstellung von Videoinhalten ist es wichtig, sowohl die Botschaft, die Sie vermitteln möchten, als auch die Art, wie diese Botschaft von Ihrer Zielgruppe aufgenommen wird, zu berücksichtigen.

Mit einem fundierten Verständnis der Werbepsychologie können Sie Videos erstellen, die die Aufmerksamkeit Ihrer Zuschauer effektiver auf sich ziehen und deren Verhalten positiv beeinflussen.

In diesem Artikel zeigen wir Ihnen, wie Sie Werbepsychologie einsetzen können, um Ihr Videomarketing entscheidend voranzubringen. Konkret beleuchten wir vier wirkungsvolle verkaufspsychologische Techniken, um Ihre Videos zu optimieren:

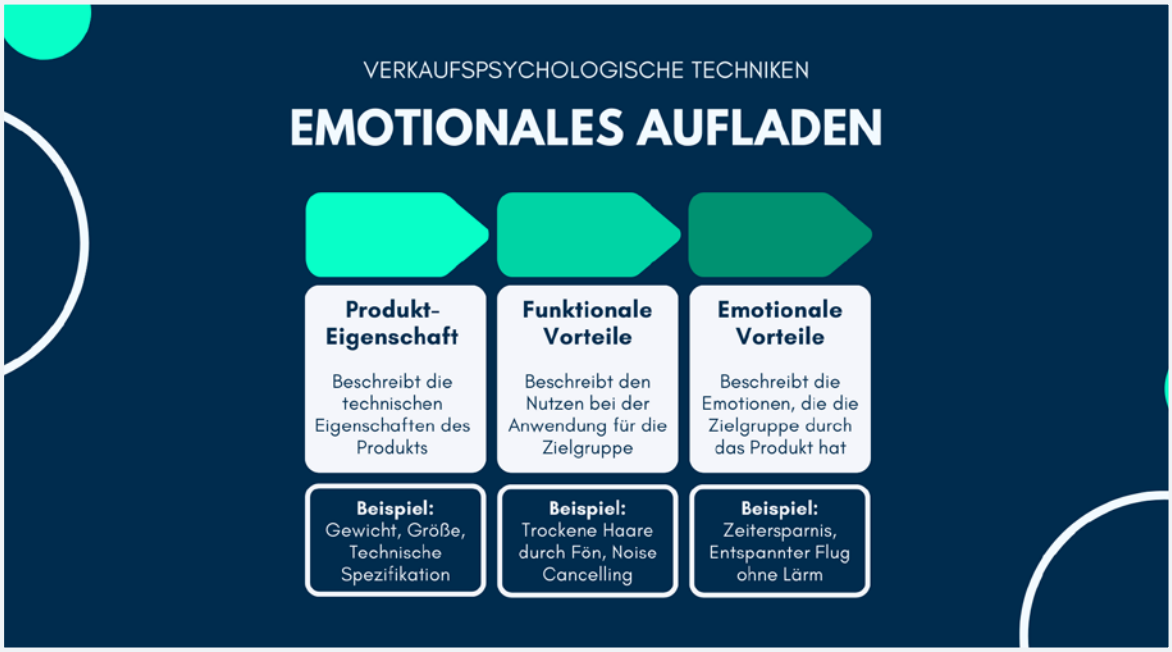
1. die Kraft des **emotionalen Aufladens**
2. die Wirkungsweise des **Mere-Exposure-Effekts**
3. den gezielten Einsatz von **heuristischen Abkürzungen**
4. die Erstellung von **wirkungsvollen Headlines**

Mit dem gezielten Einsatz dieser vier verkaufspsychologischen Techniken ist das Erstellen konversionsstarker Videos eine Leichtigkeit. Ganz gleich, ob Sie ein Video für eine Produkteinführung, eine Videobiografie für ein Vorstellungsgespräch oder die ideale Instagram Reel Ad erstellen möchten.

Technik Nr. 1: Emotionales Aufladen – Steigern Sie die Effektivität Ihres Videomarketings mithilfe gefühlsbetonter Sprache

Emotional aufgeladene Sprache ist ein mächtiges Werkzeug im Videomarketing. Mit sorgfältig formulierten Botschaften können Sie die tiefsten Wünsche und Sehnsüchte Ihrer Zielgruppe ansprechen und diese zum Handeln motivieren.

Um Videos zu erstellen, die eine mitreißende Sprache verwenden, müssen Sie die Emotionen Ihrer Zielgruppe genau kennen. Welche Wünsche und Werte hat Ihr Publikum? Welche Ängste und Zweifel hegen sie? Indem Sie die Emotionen Ihrer Zielgruppe verstehen, können Sie Ihre Sprache so anpassen, dass Adressaten auf einer tiefen Ebene angesprochen werden.



Infografik über die drei Schritte des emotionalen Aufladens. © Erklärhelden

Nachdem Sie die Emotionen Ihres Zielpublikums identifiziert haben, können Sie eine Redeweise, die diese explizit anspricht, gezielt verwenden. Hier sind einige Tipps:

- Verwenden Sie eine **sinnliche Sprache**, damit Ihr Publikum sich die Emotionen vorstellen kann, die Sie vermitteln wollen. Statt „unser Produkt ist effektiv“ lieber „unser Produkt macht Sie selbstbewusst und unwiderstehlich“.

- Verwenden Sie **Powerwörter**, die starke Emotionen hervorrufen. Zum Beispiel sind „revolutionär“ oder „lebensverändernd“ starke Ausdrücke, die Zuschauer begeistern und motivieren können.

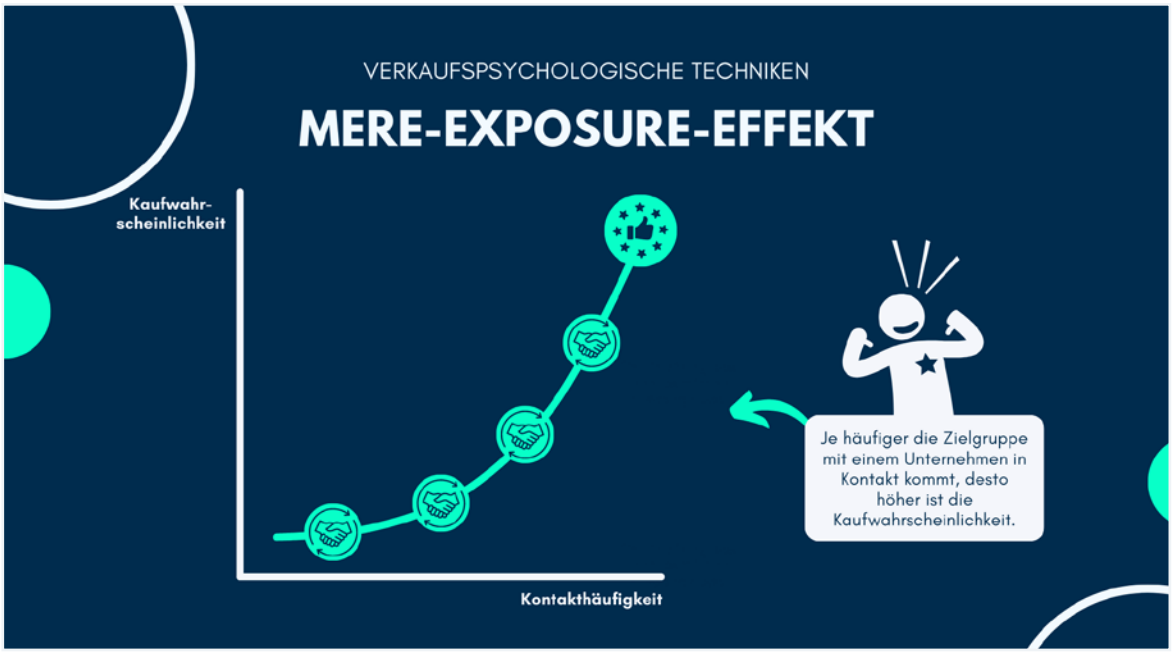
- Verwenden Sie eine **positive Sprache**, um ein Gefühl von Optimismus zu vermitteln. Anstatt „Unser Produkt wird Sie vor dem Scheitern bewahren“ lieber „Unser Produkt wird Ihnen zum Erfolg verhelfen“.

- Verwenden Sie **Dringlichkeit**, um ein Gefühl der Verknappung zu erzeugen. „Befristetes Angebot“ oder „noch bis zum Montag verfügbar“ sind hervorragende Formulierungen, die Dringlichkeit erzeugen und zum Kauf anregen.

Technik Nr. 2: Der Mere-Exposure-Effekt – Kreieren Sie herausragende Videos durch gezielte Wiederholungen

Der Mere-Exposure-Effekt ist ein psychologisches Phänomen, das beschreibt, wie Menschen eine Vorliebe für Dinge entwickeln, die ihnen vertraut erscheinen. Im Videomarketing kann dieser Effekt genutzt werden, um konversionsstarke Videos zu erstellen, die Ihr Zielpublikum genau ansprechen.

Wiederholung ist der entscheidende Faktor für den erfolgreichen Einsatz des Mere-Exposure-Effekts im Marketing. Menschen entwickeln eher eine Präferenz für Produkte, mit denen sie mehrfach in Berührung kommen. Achten Sie bei der Erstellung von Marketingvideos darauf, dass Ihr Produkt in mehreren Szenen vorkommt sowie in verschiedenen Zusammenhängen gezeigt wird. So kommen die Zuschauer*innen häufiger mit Ihrem Produkt in Kontakt und lernen es besser kennen.



Mit zunehmenden Kontaktpunkten steigt auch die Kaufwahrscheinlichkeit. © Erklärhelden

Allerdings sollte die Wiederholung nicht aufdringlich wirken. Ausgezeichnetes Marketing geschieht unauffällig. Nutzen Sie subtiles Branding, um Ihre Produkte in Ihren Videos besser zu präsentieren. Sie könnten etwa Ihr Produkt im Hintergrund einer Szene platzieren oder jemanden zeigen, der es auf natürliche Art und Weise benutzt. So können sich Kunden und Kundinnen mit Ihrem Produkt vertraut machen, ohne das Gefühl zu bekommen, plumpen Werbebotschaften ausgesetzt zu sein.

Eine weitere Möglichkeit: Die dauerhafte Einblendung des Logos oder der Domain in einer Bildecke. Das hat einen starken Branding-Effekt und spricht gleichzeitig das Unterbewusstsein der Zuschauer*innen an.

Technik Nr. 3: Heuristiken – Nutzen Sie Abkürzungen des Gehirns, um konversionsstarke Videos zu erstellen

Wenn es um effektives Marketing geht, können Heuristiken ein mächtiges Werkzeug sein. Heuristiken sind mentale Abkürzungen, die Menschen verwenden, um schnell und effizient Entscheidungen zu treffen.

> Der Framing-Effekt ist eine bekannte Heuristik. Er besagt, dass Entscheidungen von Menschen stark von der Art und Weise der Informationspräsentation beeinflusst werden. Achten Sie daher auf positiv besetzte Wörter und Bilder.

Indem Sie verstehen, wie Heuristiken funktionieren, können Sie diese nutzen, um konversionsstarke Videos zu erstellen. Hier sind einige Tipps, wie Sie Heuristiken beim Erstellen von Werbevideos effektiv einsetzen können.

- Verwenden Sie **Social Proof**. Social Proof besagt, dass Menschen eher den Handlungen Anderer folgen. Bauen Sie Erfahrungsberichte oder Bewertungen von Kunden und Kundinnen in Ihre Marketingvideos ein. Zeigen Sie echte Menschen, die Ihr Produkt verwenden und davon profitieren, um Glaubwürdigkeit und Vertrauen zu schaffen.

- Konzentrieren Sie sich auf Vorteile, nicht auf Merkmale. Die **Feature-Advantage-Benefit-Heuristik** besagt, dass Menschen eher von den Vorteilen eines Produkts angesprochen werden als von seinen Eigenschaften. Anstatt sich nur auf die technischen Spezifikationen Ihres Produkts zu konzentrieren, betonen Sie, wie es das Leben Ihrer potenziellen Kunden verbessern kann.

- Die **Verknappungsheuristik** besagt, dass Menschen Dingen, die selten oder schwer zu bekommen sind, einen höheren Wert beimessen. Um die Verknappungsheuristik in Ihren Marketingvideos zu nutzen, weisen Sie auf zeitlich begrenzte Werbeaktionen oder exklusive Angebote hin. Dies kann ein Gefühl der Dringlichkeit erzeugen und potenzielle Kundschaft dazu ermutigen, schnell zu handeln. Alternativ können Sie auch einem bestimmten Kundenkreis Vorabzugang geben oder ein geschlossenes Bonusprogramm bewerben.

- Verwenden Sie den **Ankereffekt**. Der Ankereffekt besagt, dass sich Menschen bei einer Entscheidung stark auf die erste Information verlassen, die sie erhalten. Beginnen Sie mit einer starken Einleitung, die die Aufmerksamkeit Ihres Publikums fesselt. Dies kann den Ton für den Rest des Videos vorgeben und dazu beitragen, die Wahrnehmung Ihrer Marke zu festigen.

Technik Nr. 4: Wirkungsvolle Headlines – Verleihen Sie Ihren Videos aussagekräftige Titel

Es reicht nicht aus, ein großartiges Marketingvideo zu erstellen, um potenzielle Zuschauer anzulocken. Eine aufmerksamkeitsstarke Headline, die dazu verleitet, Ihren fantastischen Content anzusehen, ist unerlässlich. Die drei wichtigsten Tipps für eine wirkungsvolle Headline:

- Ihre Headline sollte **prägnant** sein. Beschränken Sie sich auf etwa acht bis vierzehn Wörter, damit Ihre Headline verständlich ist und in Suchergebnissen nicht abgeschnitten wird.

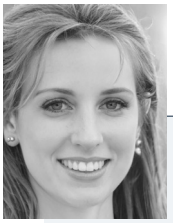
- Menschen treffen Entscheidungen auf der Grundlage von **Emotionen**. Verwenden Sie daher positive Wörter wie „glücklich", „selbstbewusst" oder „erfolgreich" in Ihrer Headline, um Ihre Zielgruppe anzusprechen.

- Die Verwendung von **Keywords** in Ihrer Headline ist entscheidend für die Suchmaschinenoptimierung (SEO). Ihre Headline sollte einschlägige Keywords enthalten, nach denen Ihr Zielpublikum sucht.

Fazit

Die Verwendung von verkaufspsychologischen Techniken in Videos kann insbesondere für Unternehmen, die ihre Produkte oder Dienstleistungen online verkaufen, einen erheblichen Vorteil bringen. Durch die Schaffung von sozialer Bewährtheit und die Verwendung von Emotionalität können potenzielle Kunden und Kundinnen dazu gebracht werden, sich mit den Leistungen zu identifizieren und sie als Lösung für ihre Probleme zu sehen.

Unternehmen sollten sich bemühen, diese Techniken in ihre Videoinhalte zu integrieren, um ihre Konversionsraten zu erhöhen und ihre Verkaufszahlen zu steigern.



AUTORIN

Katharina Schneider

Konzepterin bei der Erklärhelden GbR

Katharina Schneider ist als Konzepterin bei der Berliner Erklärvideo-Agentur Erklärhelden tätig. Dort ist sie für das Storytelling von überzeugenden Erklärfilmen verantwortlich und besitzt durch ihre Erfahrung in der Produktion von audiovisuellem Content ein fundiertes Wissen darüber, wie Zielgruppen erfolgreich angesprochen werden können. Ein Leitfaden zum Erstellen von Erklärvideos kann hier abgerufen werden.

www.erklaerhelden.de
Katharina Schneider auf LinkedIn

Das vorliegende Magazin ist eine kostenlose Publikation von:

TechDivision GmbH
An der Alten Spinnerei 2a
83059 Kolbermoor
Tel. +49 8031 221055-0
Fax +49 8031 221055-22
E-Mail: info@techdivision.com
www.techdivision.com

Redaktion

Herausgeber & Chefredakteur (Für den Inhalt verantwortlich)
Josef Willkommer
j.willkommer@estrategy-magazin.de

Eva Hausruckinger
e.hausruckinger@estrategy-magazin.de

Christian Markuz
c.markuz@estrategy-magazin.de

Freie Autoren:
Tobias Schlotter, Kateryna Kaida, Michael Froment, Franz Xaver Obermayer, Marcus Döllerer, Rico Barth, Viktoria Grimm, Sebastian Gerstl, Dr. Christian Schunck, Antonia Breitenfellner, Alexander Friedrich, Katerina Arsova, Olaf Brandt, Benoit Jacquemont, Hartmut König, Katharina Schneider

Grafik, Design & Layout
Sandro Lindner – Büro für Marketing und Design

Lektorat
Claudia Sarkady (claudia.sarkady@t-online.de)
Josef Grabmayr (jg@cg8.eu)

Weitere Informationen erhalten Sie auf dem Webauftritt unter:
www.estrategy-magazin.de

Anzeigen
werbung@estrategy-magazin.de
Tel. +49 8031 221055-0
Fax +49 8031 221055-22

Pressemitteilungen
pressemeldungen@estrategy-magazin.de

Urheberrecht
Die im eStrategy-Magazin erschienenen Beiträge sind urheberrechtlich geschützt. Alle Rechte, auch Übersetzungen, sind vorbehalten. Die Reproduktion jeglicher Art, egal ob Fotokopie, Mikrofilm oder Erfassung in Datenverarbeitungsanlagen, kann nur mit schriftlicher Genehmigung des Herausgebers erfolgen. Aus der Veröffentlichung kann nicht geschlossen werden, dass die beschriebene Lösung oder verwendete Bezeichnung frei von gewerblichen Schutzrechten sind.

Haftung
Alle Inhalte werden sorgfältig recherchiert, dennoch können inhaltliche Fehler auftauchen. Für den Fall, dass im eStrategy-Magazin unzutreffende Informationen in Beiträgen oder Fehler in Werbeanzeigen enthalten sind, kommt eine Haftung nur bei grober Fahrlässigkeit des Herausgebers oder seiner Mitarbeiter in Betracht. Bitte beachten Sie, dass für unaufgefordert eingesandte Manuskripte, Datenträger, Produkte und Fotos keine Haftung übernommen wird. Grundsätzlich können auch nur elektronisch versante Dokumente und Inhalte berücksichtigt werden.

Alle verwendeten Logos & Grafiken sind Eigentum der jeweiligen Unternehmen.