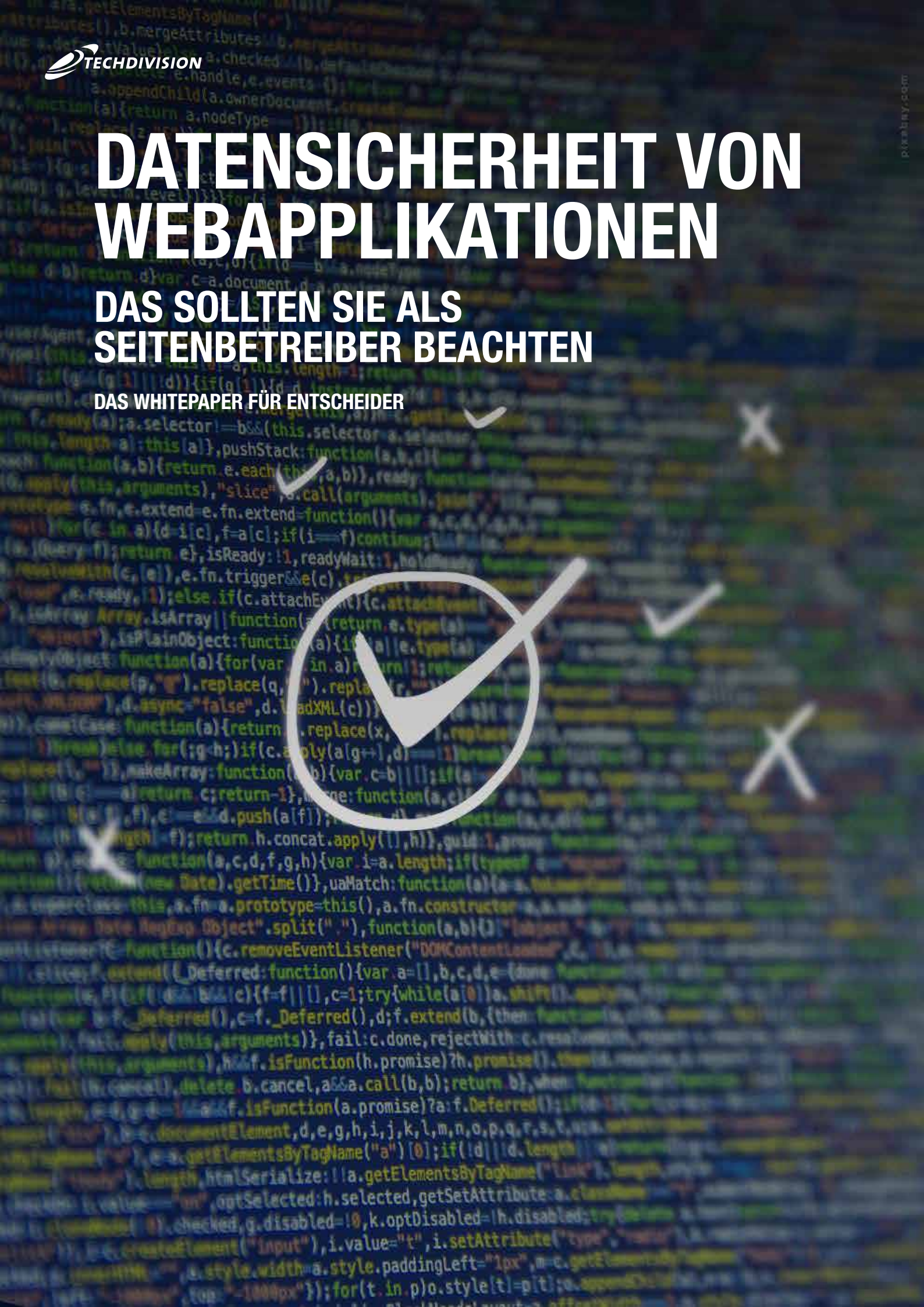
TECHDIVISION

DATENSICHERHEIT VON WEBAPPLIKATIONEN

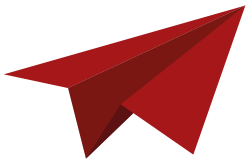
DAS SOLLTEN SIE ALS SEITENBETREIBER BEACHTEN

DAS WHITEPAPER FÜR ENTSCHEIDER



TECHDIVISION

DATENSICHERHEIT VON WEBAPPLIKATIONEN ALS EINES DER TOP-THEMEN 2017



Das Thema Security hat im letzten Jahr ja bereits zu Recht deutlich an Fahrt aufgenommen und 2017 wird das Ganze nach unserer Meinung zu einem der Top-Themen werden. Mittlerweile gibt es sogar gesetzliche Pflichten zum Einspielen von Patches und Updates für Webseitenbetreiber, allerdings ist das Verständnis und die Bereitschaft für eine permantene Wartung und Pflechte von Webapplikationen – egal ob CMS, Online-Shop oder sonstiger Applikation und auch vollkommen unabhängig von der verwendeten Technologie – bei Unternehmen häufig nur begrenzt vorhanden.

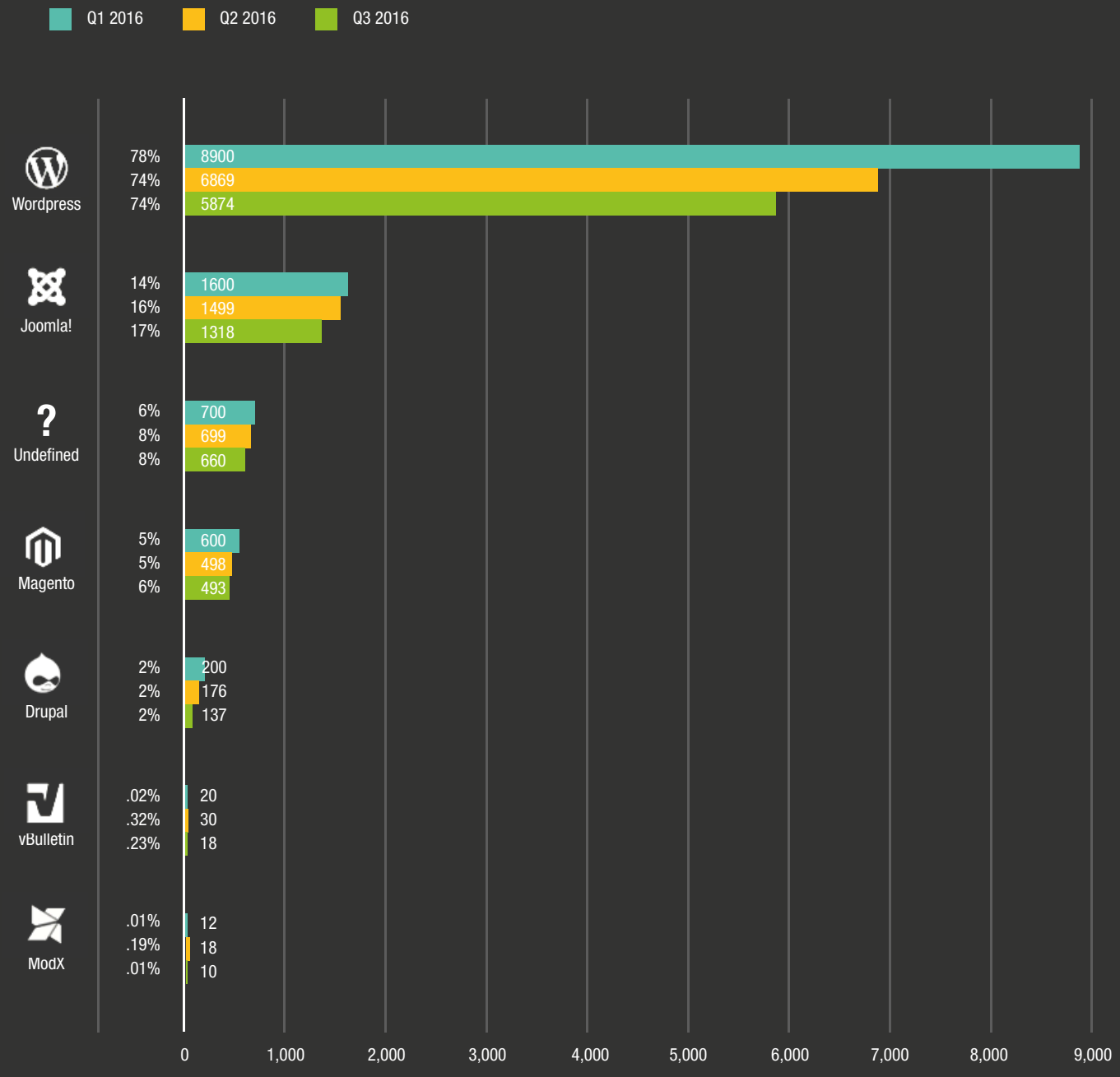
Aus unserer Sicht ist es absolut richtig, dass das Thema Datensicherheit immer stärker in den Fokus rückt - zumal Seitenbetreiber ja auch für die Sicherheit ihres Webangebotes verantwortlich sind. Dennoch scheint es hier aktuell noch eine „Zwei-Klassen-Gesellschaft“ zu geben: Die Einen haben das Thema mit entsprechender Priorität und proaktiv auf ihrer Agenda, die Anderen sehen das eher locker und unternehmen – wenn überhaupt - erst etwas, wenn echte Gefahr droht oder noch schlimmer, erst dann wenn etwas passiert ist.
Aktuell geistern wieder diverse Meldungen über die Sicherheit von (Web-)Applikationen durch die Fachmedien. Zum Teil wird da mit recht reisserischen Überschriften hantiert ohne eine tiefergehenderen Blick auf die Fakten.

TECHDIVISION

HEUTE MAGENTO UND MORGEN DIE NÄCHSTE TECHNOLOGIE

Erst die Tage kam wieder eine Meldung, dass rund 1.000 deutsche Online-Shops durch eine Sicherheitslücke in der Shopsoftware – in diesem Fall handelte es sich um Magento - gehackt wurden und gleich lief dazu die Medien-Maschinerie an. So wurde unter anderem auch immer wieder auf den „Hacked Website Report Q3 2016“ des IT-Security Unternehmen Sucuri verwiesen. Demnach führt das CMS Wordpress dieses unrühmliche Ranking mit massivem Abstand an, gefolgt von Joomla und Magento. Warum Wordpress hier so „dick“ dabei ist, lässt sich mit dem Marktanteil der Software erklären. Bei Wordpress handelt es sich um das mit exorbitantem Abstand am weitesten verbreitete CMS weltweit. Glaubt man den Analysen und Daten von Wordpress läuft rund ein Viertel aller Websites (!!!) auf Wordpress. Die Zahlen kann man jetzt glauben oder nicht. Fakt ist, dass Wordpress im Bereich Content Management Systeme extrem weit verbreitet ist. Von daher ist es auch nur logisch, dass bei einer derartigen Verbreitung – insbesondere im Hobby- und Semi-Professionellen-Bereich - auch die Wahrscheinlichkeit etwaiger Angriffe deutlich größer als bei anderen Systemen ausfällt, d.h. es besteht eine deutliche Korrelation zwischen der Anzahl an Installationen und möglichen Angriffen.

INFECTED WEBSITES PLATFORM DISTRIBUTION Q3 -2016



Quelle: Sucuri

Mit Joomla und Drupal folgen weitere „echte“ CMS mit signifikantem Abstand. Dass Magento hier als CMS geführt wird, entzieht sich unserer Kenntnis da es doch gravierende Unterschiede zwischen einem klassischen CMS und einer Shopsoftware gibt. Magento ist das weltweit führende Shopsystem, das bei rund 250.000 Shops im Einsatz ist. Ein Online-Shop bildet dabei für Hacker in den meisten Fällen ein deutlich interessanteres Angriffsziel, als eine „normale“ Webseite, da hier Zahlungen und Zahlungsdaten transferiert werden - es geht also um Kohle und das häufig nicht zu knapp.

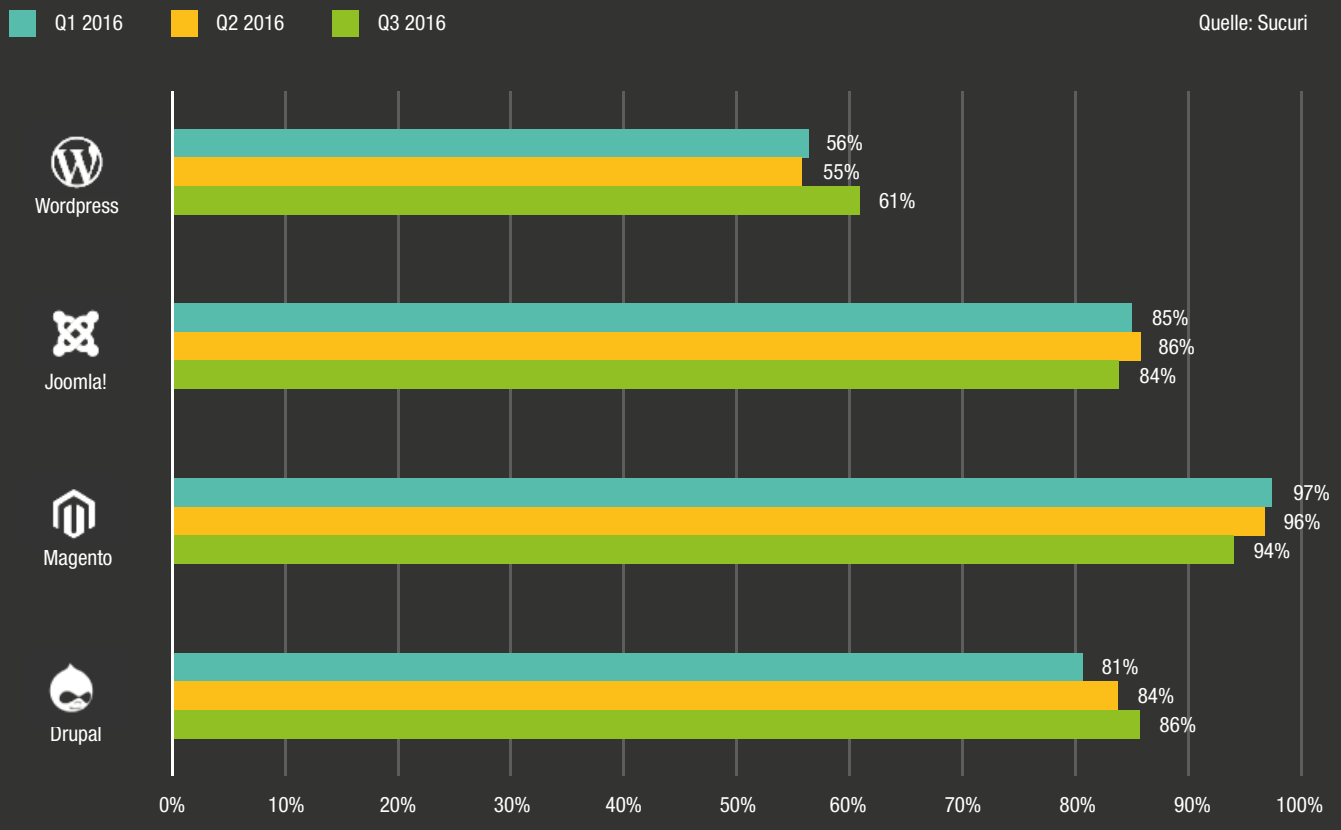
FEHLENDE UPDATES ALS ZENTRALES PROBLEM

Keine Software dieser Welt ist fehlerfrei und es ist immer nur eine Frage des Aufwands, um sich Zugang zu entsprechenden Daten zu verschaffen. Zukünftig wird dies tendenziell auch nicht weniger werden. Daher gibt es sowohl für Open Source- als auch Proprietäre Software Security Teams, die das Thema Datensicherheit bearbeiten und sich permanent um die Behebung auftauchender Sicherheitslücken kümmern. Die im Falle von Magento angesprochene Sicherheitslücke wurde bereits im September 2016 bekannt und Magento hat hier sehr schnell und professionell mit entsprechenden Patches und einer klaren Kommunikation reagiert.

Wenn jetzt nach mehrere Monaten noch immer entsprechend viele Online-Shops nicht gepatcht wurde, muss man hier primär dem Shopbetreibern bzw. ggf. dem verantwortlichen Dienstleister den „schwarzen Peter“ zuschieben und hier massive Versäumnisse attestieren.

Dass im aktuellen Magento-Fall genau dieses Szenario zum tragen kommt bzw. kam zeigt ein Blick auf betroffene Shops. Im überwiegenden Fall handelt es sich hier um kleinere Hobby- und Bastel-Shops die auf einer älteren Standard-Installationen basieren und zwischenzeitlich nicht auf den aktuellen Stand gebracht wurden. In der Analyse von Sucuri wird dies durch folgendes Chart auch nochmals verdeutlicht. Demnach waren 94% der betroffenen Magento-Shops nicht auf dem aktuellen Softwarestand.

% OF OUT-OF-DATE CMS AT POINT OF INFECTION Q3-2016



ES BETRIFFT ALLE UNTERNEHMEN UND ALLE TECHNOLOGIEN

Der eine oder andere stellt sich anhand dieser Studie und der Tatsache, dass es sich hier jeweils um Open Source Software handelt möglicherweise die Frage: Ist Open Source Software denn nicht sicher bzw. unsicherer als proprietäre Lösungen?

Hierzu gibt es diverse „prominente“ und auch recht aktuelle Beispiele von Unternehmen, die proprietäre oder individuell programmierte Software einsetzen und dennoch gehackt wurden:

- US Wahlkampf: Das Ganze ist derzeit noch nicht bestätigt aber es gibt wohl begründete „Vermutungen“, dass russische Hacker in den Wahlkampf eingegriffen haben.
- YAHOO: Erst im September 2016 musste Yahoo den größten Hack aller Zeiten eingestehen. Nun verdichten sich die Anzeichen, dass dieselben Hacker sich bereits ein Jahr zuvor deutlich übertroffen hatten.
- Wendys: Anfang Juli 2016 wurde ein Hacker-Angriff auf die US-Fastfood-Kette Wendy’s bekannt. Auf den Kassensystemen wurde Malware gefunden. Anfangs ging man von weniger als 300 betroffenen Filialen aus, wobei am Ende dann doch rund 1.000 Filialen auf der Uhr standen.
- J.P. Morgan Chase: Mit J.P. Morgan rückte im Juli 2014 eine der größten US-Banken ins Visier von Cyberkriminellen. Dabei erbeuteten die Hacker rund 83 Millionen Datensätze von Kunden.
- ADOBE: Mitte September 2013 wurde Adobe das Ziel von Hackern. Circa 38 Millionen Datensätze von Adobe-Kunden wurden im Zuge des Cyberangriffs gestohlen - darunter die Kreditkarteninformationen von knapp drei Millionen registrierter Kunden.
- SONY Playstation: Im April 2011 ging bei vielen Playstation-Besitzern rund um den Globus nichts mehr, da das digitale Serviceportal gehackt wurde und Daten von rund 77 Mio. Kunden gestohlen wurden.

Die Liste ließe sich dabei beliebig verlängern und zeigt doch recht deutlich, dass wir uns hier zukünftig noch auf einiges gefasst machen müssen. Der Bankräuber von heute stürmt nicht mehr bewaffnet in ein Gebäude. Häufig sitzt er inzwischen vor dem heimischen PC irgendwo auf der Welt und ist mitunter noch nicht mal Volljährig! Das Ganze funktioniert allerdings auch noch deutlich professioneller und in größerem Stil...
Insofern muss man ganz klar argumentieren, dass es am Ende des Tages auch vollkommen egal ist, welche Tools und Technologien eingesetzt werden. Das Thema Datensicherheit betrifft alle und muss jeweils oberste Priorität haben.
Moderne Open Souce Software ist bei richtiger Verwendung nicht unsicherer als proprietäre Lösungen. Im Gegenteil: Aufgrund der Verbreitung und der häufig sehr großen Community werden etwaige Sicherheitslecks in der Regel schneller geschlossen, als dies bei proprietärer Software der Fall ist.
Laut einer Studie des Ponemon-Instituts aus dem Jahr 2015 sind zum Beispiel zwei Drittel der rund 1.400 befragten IT-Entscheider und Sicherheitsexperten davon überzeugt, dass Open Source die Sicherheit von Anwendungen erhöht – und zugleich den Schutz privater Daten verbessert. Ein weiteres Ergebnis der Studie: Die allgemeine Zuverlässigkeit von Software-Anwendungen werde durch die Transparenz des Programmcodes und durch den Support kommerzieller Open-Source-Anbieter erhöht. Das gaben 75 Prozent der Befragten an.

SOFTWARE BRAUCHT PERMANENTE WARTUNG UND PFLEGE

Des deutschen liebstes Kind, das Auto, muss in gewissen Abständen zur Inspektion und zum TÜV und selbst hier muss inzwischen immer häufiger auch mal ein Update eingespielt werden. Erfolgt dies nicht kann dies ernsthafte Konsequenzen nach sich ziehen. Bei echter (Web-)software verhält sich das ganz genau so - mit dem Unterschied, dass es hier aktuell immer noch sehr häufig zu großen Diskussionen bzw. Unverständnis kommt. Hier ist aus unserer Sicht massives Umdenken angesagt und IT-Verantwortliche sollten gerade im Blick auf die Zukunft verstärkt in IT-Sicherheit investieren. Selbst wenn laut ihrer Auffassung ihr Unternehmen kein interessantes Angriffsziel darstellt: Hackern ist es mitunter auch egal, ob und was hier ggf. zu holen ist. Hier geht es auch nur mal ums ausprobieren und „spielen". Wenn durch solche „Spielchen" ihre IT lahm gelegt wird, hat das in der heutigen Zeit in nahezu allen Branchen und Bereichen mitunter massive Auswirkungen und entstehen darüberhinaus in aller Regel auch Aufwände, die schnell recht unangenehm werden können – deutlich teurer als ein permanentes Investment in Wartung und Pflege.

Wir haben hierzu mit dem Fachanwalt für IT-Recht, Dr. Matthias Orthwein von der Kanzlei SKW Schwarz zu diesem Thema gesprochen. Nachfolgend erhalten Sie einige wichtige Hinweise und Tipps zum Thema Datensicherheit:

1 WARUM MUSS EIN WEBSHOP AKTUALISIERT WERDEN, AUCH WENN ER PROBLEMLOS LÄUFT – GILT NICHT „NEVER TOUCH A RUNNING SYSTEM"?

Die regelmäßige Anpassung von Unternehmenssoftware ist ein Gebot der Vernunft, insbesondere bei unternehmenskritischen Anwendungen wie dem Online Shop. Wer da nicht auf dem aktuellen Stand bleibt, verhält sich wie der Autofahrer, der mit abgefahrenem Profil über die Autobahn fährt: Er kommt vorwärts, aber wehe er muss am Stauende bremsen…
Mittlerweile gibt es sogar gesetzliche Pflichten zum Einspielen von Patches und Updates für Webseitenbetreiber. § 13 Abs. 7 Telemediengesetz (TMG) verlangt von allen Webseitenbetreibern die Beachtung zumindest eines Standard-Sicherheitsniveaus, wie es jeweils aktuell üblich ist und verlangt werden kann. Dazu gehören insbesondere das Einspielen aktueller Patches und die Verwendung aktueller Software, in vielen Fällen auch der umfassende Einsatz wirksamer Verschlüsselungstechnologien. Auch der Schutz der Verfügbarkeit von Daten z.B. gegen DOS Attacken oder Ransomsoftware durch regelmäßige Backups und eine abgesicherte redundante Infrastruktur sind zu gewährleisten. Das Gesetz verlangt eine Umsetzung aller technisch möglichen und wirtschaftlich zumutbaren Maßnahmen.
Wirtschaftliche Überlegungen zum finanziellen Aufwand beim Einspielen von Softwareupdates dürfen in der Planung zwar durchaus eine Rolle spielen. Solange der Aufwand allerdings nicht vollständig unverhältnismäßig und unzumutbar ist, taugen solche Überlegungen nicht als Entschuldigung, den Onlineshop nicht zeitnah auf aktuellem Stand der Sicherheitstechnik zu halten.
Praktische Hinweise zur Umsetzung des gesetzlichen Maßstabs finden sich im Leitfaden des Bundesamts für Sicherheit in der Informationstechnologie (BSI) https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_125.html

2 MÜSSEN NUR MAGENTO ONLINESHOPS AKTUALISIERT WERDEN?

Die Pflicht zur Verwendung aktueller Software und eines aktuellen Stand der Sicherheitstechnik richtet sich keineswegs nur an Verwender einzelner Softwareprodukte, sondern vielmehr an jeden, der eine Webseite oder einen Onlineshop mit einer gewissen Nachhaltigkeit und Gewinnerzielungsabsicht betreibt. In der Praxis gilt dies für alle Onlineshops und nahezu alle Webseiten, die von Unternehmen betrieben werden. Diese Pflicht gilt technologieunabhängig und für alle online erreichbaren Kanäle, also z.B. auch für mobilen Zugriff optimierte Angebote.
Selbst private Websites oder Vereinsseiten, die die Zuschaltung von Werbebannern zulassen, sollen dem Gesetz unterfallen. Nur wer ausschließlich auf den Plattformen Dritter (z.B. Facebook oder Xing) seine Angebote online stellt, kann sich darauf zurückziehen, dass der Plattformbetreiber für die Sicherheit seiner Plattformsoftware selber verantwortlich ist.

3 GENÜGT ES NICHT, WENN DER SOFTWARE-HERSTELLER SICH UM DAS PROBLEM KÜMMERT?

In der Tat sind insbesondere die Softwarehersteller aufgefordert, das Schicksal ihrer Produkte gegenüber aktuellen Sicherheitsbedrohungen zu beobachten und ggf. durch Patches oder Updates und Warnungen auf neu erkannte Bedrohungen zu reagieren. Daher hat im konkreten Fall ja auch Magento direkt nach Bekanntwerden der Schwierigkeiten im Herbst 2016 umfassend reagiert.
Wichtig ist dann aber, dass die Anwender der Software diese Herstellerinformationen auch ernst nehmen und bereitgestellte Hilfsmittel und Patches unverzüglich einspielen bzw. einspielen lassen.

4 WAS PASSIERT, WENN EIN ONLINESHOP NICHT AKTUALISIERT WIRD?

Bei Verstoß gegen die allgemeine Pflicht zur Beachtung aktueller Sicherheitsstandards und zur Verwendung des aktuellen Stands der Softwareabsicherung drohen Bußgelder bis zu EUR 50.000 und mittelbar mögliche Schadensersatzansprüche von Nutzern, deren Daten z.B. aufgrund nicht rechtzeitig geschlossener Sicherheitslücken gehackt und unrechtmäßig genutzt wurden.

5 WAS MUSS DER ONLINESHOP BETREIBER TUN, WENN ER EINEN EINBRUCH IN DEN ONLINESHOP FESTSTELLT?

Nach heute geltendem Recht müssen illegale Zugriffe auf besonders sensible Daten wie z.B. Bank-/ Kredikartendaten sowohl dem Betroffenen als auch der zuständigen Datenschutzaufsichtsbehörde unverzüglich gemeldet werden (§ 42a Bundesdatenschutzgesetz, BDSG). In der Praxis bedeutet dies, dass üblicherweise innerhalb von 48 Stunden eine Meldung sowohl an die Behörde als auch an die Kunden erfolgen sollte. Allerdings eben nur, wenn auch wirklich solche sensiblen Daten betroffen sind. Der reine Klau von Benutzernamen und Passwörtern musste bisher nicht unbedingt immer und sofort gemeldet werden.
Dies ändert sich mit dem neuen europaweit geltenden Datenschutzrecht ab 2018. Mit dem Wirksamwerden der Datenschutzgrundverordnung am 25. Mai 2018 müssen künftig alle Verletzungen des Schutzes personenbezogener Daten (egal ob Bankdaten oder Postanschrift) innerhalb einer festen Frist von höchstens 72 Stunden der Datenschutzaufsichtsbehörde gemeldet werden (Art. 33 DS-GVO). Auch die Betroffenen sind weiterhin zu informieren, es sei denn, der Webseitenbetreiber kann einen Schaden für seine Kunden (z.B. durch Identitätsklau etc.) ausschließen. Auch hier spielen wieder technische Vorsorgemaßnahmen wie der Einsatz von wirksamen Verschlüsselungen eine Rolle, um Schäden verlässlich ausschließen zu können.

DARAUF SOLLTEN SIE BESONDERS ACHTEN:

DIE NACHFOLGENDEN HINWEISE STAMMEN AUS DEM DEM VERIZON DATA BREACH INVESTIGATIONS REPORT 2015. INZWISCHEN IST DIE NACHFOLGEVERSION VERFÜGBAR (SIEHE WEITERFÜHRENDE RESSOURCEN) UND SOLLTE FÜR IT-VERANTWORTLICHE ZUR PFLICHTLEKTÜRE GEHÖREN:

- **SEIEN SIE WACHSAM**
  Unternehmen erfahren oft erst von Sicherheitsverletzungen, wenn sie einen Anruf von der Polizei oder einem Kunden erhalten. Log-Dateien und Change-Management- bzw. Monitoring-Systeme können Sie frühzeitig warnen.

- **HÄUFIG SITZT DIE „SCHWACHSTELLE“ VOR DEM RECHNER**
  Sensibilisieren Sie Ihre Mitarbeiter für das Thema Sicherheit – hierzu gehört auch der Zugang zu Rechner und IT-Systemen. Schulen Sie sie darin, die Anzeichen eines Angriffs zu erkennen und richtig zu reagieren, wenn sie etwas Verdächtiges sehen.

- **BEGRENZEN SIE DEN ZUGANG ZU IHREN DATEN AUF DAS GESCHÄFTLICH NOTWENDIGE**
  Grenzen Sie den Zugriff auf die Systeme ein, die das Personal für die Ausübung seiner Tätigkeiten benötigt. Stellen Sie sicher, dass Prozesse etabliert sind, die dafür sorgen, dass Mitarbeiter ihre Zugriffsrechte verlieren, wenn sie andere Aufgaben übernehmen oder das Unternehmen verlassen.

- **BEHEBEN SIE SOFTWAREFEHLER UNVERZÜGLICH**
  Sie können Sich gegen viele Angriffe allein dadurch schützen, dass Sie sicherstellen, dass Ihre IT-Umgebung sorgfältig konfiguriert ist und die Virenschutz-Programme aktuell sind.

- **HALTEN SIE IHRE SOFTWARE AKTUELL**
  Durch regelmäßige Softwareupdates sowie das Einspielen etwaige Patches können Sie das Ausnutzen bekannter Sicherheitslücken in ihren Systemen vermeiden.

- **VERSCHLÜSSELN SIE SENSIBLE DATEN**
  Das wird den Diebstahl sensibler Daten nicht verhindern, aber es wird es Kriminellen wesentlich schwerer machen, etwas damit anzufangen.

- **VERWENDEN SIE DIE ZWEI-FAKTOR-AUTHENTIFIZIERUNG**
  Dadurch wird das Risiko eines Diebstahls von Passwörtern nicht verringert, es kann jedoch der Schaden begrenzt werden, der durch verlorene oder gestohlene Zugangsdaten entstehen kann.

- **VERGESSEN SIE DIE PHYSISCHEN SICHERHEITSVORKEHRUNGEN NICHT**
  Nicht alle Diebstähle geschehen online. Kriminelle machen sich an Computern oder Zahlungsterminals zu schaffen oder stehlen Kartons mit Ausdrucken.

- **WEITERFÜHRENDE RESSOURCEN:**
  > http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
  > https://blog.sucuri.net/2017/01/hacked-website-report-2016q3.html
  > https://w3techs.com/technologies/overview/content_management/all
  > https://www.owasp.org/index.php/Main_Page
  > https://en.wikipedia.org/wiki/Web_application_security

TECHDIVISION

DAS TECHDIVISION ANGEBOT

Wenn Sie sich jetzt unsicher im Bezug auf Securitythemen ihrer Magento-, TYPO3- oder Individual-Applikation sind, können Sie sich jederzeit gerne mit uns in Verbindung setzen. Gerne beraten wir Sie hierzu kostenlos und unverbindlich. Im Rahmen detaillierter Audits prüfen wir ihre bestehende Software unter anderem auch in Bezug auf etwaige Sicherheitslücken und machen konkrete Vorschläge zur Optimierung und Verbesserung. Mehr Infos zu unserem Angebot finden Sie unter:
https://www.techdivision.com/leistungen/analyse-und-beratung/magento-audit.html

AUTOREN

JOSEF WILLKOMMER, GESCHÄFTSFÜHRER TECHDIVISION

Als Geschäftsführer von TechDivision beschäftigt sich Josef Willkommer seit vielen Jahren sehr intensiv mit Themen aus den Bereichen E-Commerce, Online Marketing und den dazu notwendigen, modernen Projektmanagement-Ansätzen. Darüber ist er als Chef-Redakteur des eStrategy-Magazins – einem quartalsweise erscheinenden, kostenlosen Online-Magazin mit Fokus auf E-Commerce und Online Marketing – auch journalistisch tätig und versucht sein Wissen in Form von Fachbeiträgen weiterzugeben. Auch auf diversen Fachkonferenzen trifft man ihn als Referent zu Themen rund um den elektronischen Handel.

EXTERNE AUTOREN

Dr. Matthias Orthwein, LL.M. (Boston) /
SKW Schwarz Rechtsanwälte

ÜBER TECHDIVISION

TechDivision gehört als Magento Enterprise Partner der ersten Stunde, TYPO3 Association Gold Member zu den führenden Adressen für anspruchsvolle Webentwicklung und Digitalisierung von Geschäftsprozessen im deutschsprachigen Raum.

Unser Leistungsspektrum reicht von Consulting-leistungen über Konzept- und Designentwicklung sowie Implementierung bis hin zu Online-Marketing. Neben diversen mittelständischen Kunden vertrauen auch international agierende Unternehmen wie Allianz, Ritter-Sport, ZORO Tools, Salewa, FERRERO oder Cherry auf das Know-how und die Erfahrung von TechDivision. Aktuell verfügt TechDivision über zwei Standorte in Rosenheim/Kolbermoor und München und beschäftigt insgesamt rund 75 Mitarbeiter.

Aktuell verfügen wir über ein Magento-Team mit rund 20 zertifizierten Inhouse-Entwicklern, die über umfassende Expertise und langjährige Praxiserfahrung verfügen.

UNSER INHOUSE MAGENTO-TEAM

x4 Magento Certified Front End Developer

x1 Magento Certified Developer

x15 Magento Certified Developer Plus

x4 Magento Certified Solution Specialist

Magento 2 Trained Solution Partner

TECHDIVISION

„TURNING ONLINE PROJECTS INTO SUCCESS“

Sie haben Fragen? Wir stehen Ihnen telefonisch und per Mail gerne zur Verfügung und freuen uns auf eine gemeinsame und erfolgreiche Zusammenarbeit!

TechDivision GmbH

Spinnereiinsel 3a
83059 Kolbermoor

Balanstr. 73, Haus 8, 3 OG
81541 München

Tel +49 8031 2210 55-0
Fax +49 8031 2210 55-22

info@techdivision.com
www.techdivision.com