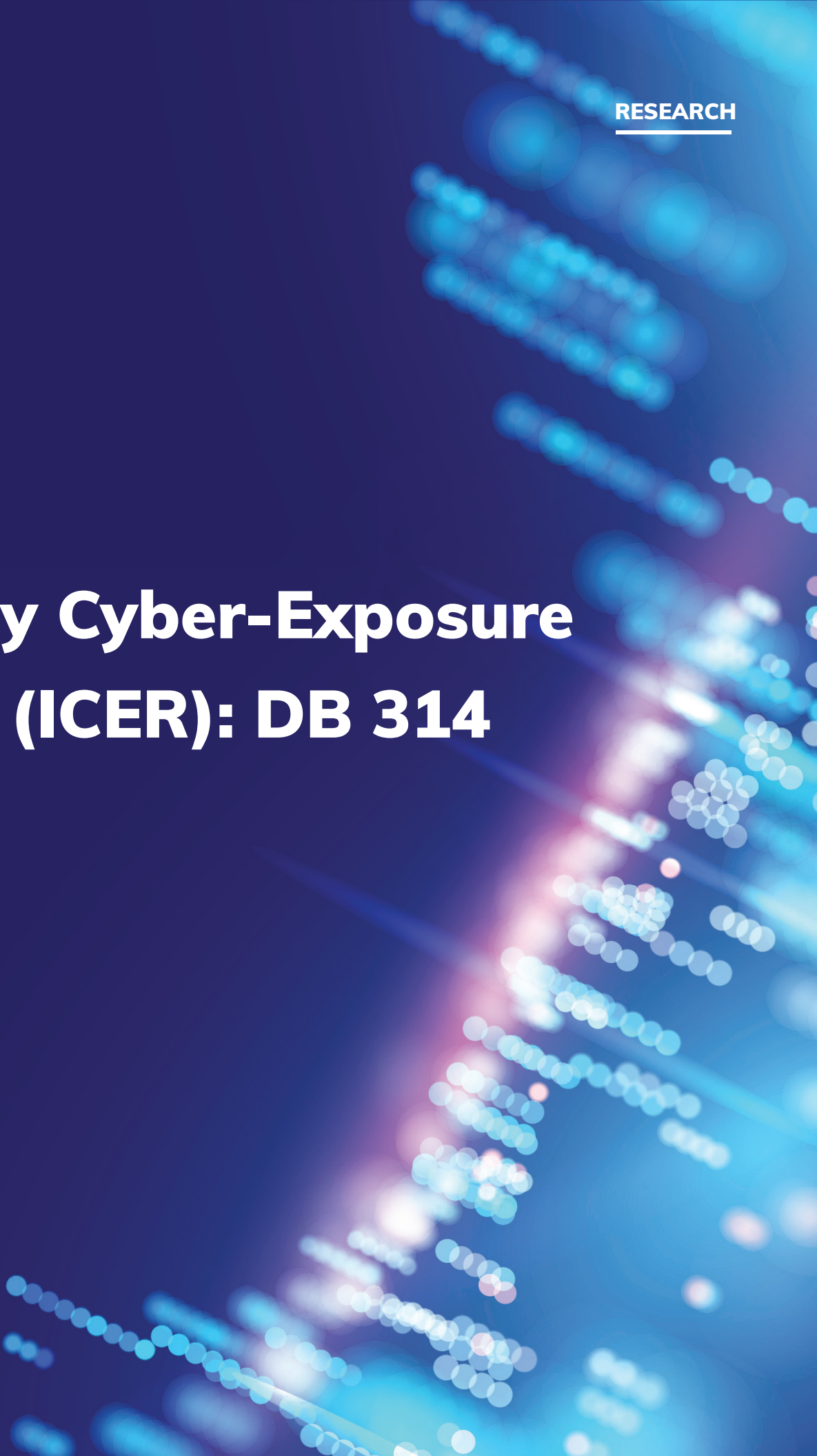
RAPID7

RESEARCH

Industry Cyber-Exposure Report (ICER): DB 314



INHALTSVERZEICHNIS

INHALTSVERZEICHNIS

Kurzfassung

Da sich die Wissensarbeiter der Welt während der Pandemie in ihre Homeoffices zurückzogen und Fälle von Ransomware im gesamten Internet kursierten, ist ein Blick auf die Internetpräsenz der bedeutendsten Unternehmen der Welt überfällig. In dieser Runde der Internet Cyber-Exposure Reports (ICERs) bewerten Forscher von Rapid7 fünf Bereiche der Cybersicherheit, die zum einen für die laufenden Geschäftsaktivitäten im und über das Internet gesichert werden müssen, und auch in die Zuständigkeit von CISOs, deren IT-Sicherheitsmitarbeiter und den internen Geschäftspartnern fallen.

Zu den fünf Aspekten der Cyber-Exponierung im Internet und der Risiken zählen:

1. Authentifizierter E-Mail-Ursprung und -Verarbeitung (DMARC)
2. Verschlüsselungsstandards für öffentliche Webanwendungen (HTTPS und HSTS)
3. Versionsverwaltung für Webserver und E-Mail-Server (Schwerpunkt auf IIS, Nginx, Apache und Exchange)
4. Für das Internet nicht geeignete, riskante Protokolle (RDP, SMB, und Telnet)
5. Verbreitung von Vulnerability Disclosure Programs (VDPs)

In diesem Bericht untersuchen wir die ins Internet gerichtete Cyber-Exposition von Spitzenunternehmen, die im Prime Standard der Deutschen Börse[1] aufgeführt sind (im Folgenden als DB 314 bezeichnet). Jeder Abschnitt enthält reale, praktische Ratschläge, die Akteure noch heute umsetzen können. Beachten Sie, dass diese Ratschläge nicht nur für CISOs gedacht sind, die Stellen in Deutsche Börse Prime Standard-Unternehmen innehaben, sondern auch für Sicherheitsexperten, die Geschäfts- und aufsichtstechnische Beziehungen mit einigen dieser renommierten Unternehmen unterhalten.

Im ersten Halbjahr 2021 wird Rapid7 Berichte veröffentlichen, die diese 5 wichtigen Grundlagenbereiche der Cybersicherheit in fünf der fortschrittlichsten Volkswirtschaften der Welt messen:

1. Fortune 500 der USA[2]
2. FTSE 350 aus Großbritannien[3]
3. ASX 200 aus Australien[4]
4. Prime Standard 314 der Deutschen Börse (dieser Bericht)
5. Nikkei 225 aus Japan

[1] https://www.deutsche-boerse-cash-market.com/dbcm-en/instruments-statistics/statistics/listes-companies
[2] https://www.rapid7.com/research/report/2021-industry-cyber-exposure-report/
[3] https://www.rapid7.com/research/reports/2021-industry-cyber-exposure-report-uk
[4] https://www.rapid7.com/research/report/2021-industry-cyber-exposure-report-anz/

Die wesentlichen Erkenntnisse

Der Bericht ist in fünf detaillierte Abschnitte unterteilt, die die oben genannten Bereiche behandeln, und die wesentlichen Erkenntnisse dieser Studie sind wie folgt:

- **Die Sicherheitslage von DB 314 liegt hinter der der USA und von Großbritannien.** Anfang 2021 kann die E-Mail-Sicherheit in der DB 314 nicht mit der vergleichbarer Unternehmen in den USA und Großbritannien mithalten. Während die Domain-based Message Authentication, Reporting & Conformance (DMARC) in den USA und in Großbritannien von rund 50 % der Unternehmen eingesetzt wird, haben nur etwa 39 % der befragten, in Deutschland tätigen Unternehmen DMARC-Einträge konfiguriert, und von diesen erhielten etwa zwei Drittel eine p=none (oder Passthrough) Richtlinie. Mit anderen Worten, nur etwa 13 % der in DB 314 aufgelisteten Unternehmen ergreifen aktive Maßnahmen, um ihre Marken, Mitarbeiter und Kunden mit DMARC p=quarantine oder p=reject Richtlinien zu schützen.

- **Exponierte, gefährliche Dienste spielen eine geringere Rolle in Deutschland.** Während gefährliche Protokoll-Exponierungen durch Windows Remote Desktop (RDP) Dateifreigabe (SMB) und Telnet weiterhin ein Problem für die befragten Unternehmen darstellen, scheint es ein nicht annähernd so großes Problem zu sein wie bei den befragten US-Unternehmen der Fortune 500: Fast 90 % der DB 314 Unternehmen meldeten keine Exponierung über RDP, SMB oder Telnet. Was darüber hinaus die sichere HTTP-Bereitstellung (HTTPS) betrifft, stellten wir fest, dass HTTPS bei 99,6 % der DB 314 Unternehmen der Standard ist (wir haben Kontakt mit dem letzten Unternehmen aufgenommen, das an HTTP festhält).

- **Nicht einheitliche Versionen stellen ein Problem dar.** Von den befragten Unternehmen, die noch ihre eigenen Microsoft Exchange-Server für das Messaging betreiben, laufen nur rund 20 % in der aktuellsten unterstützten Version, und weitere 20 % laufen in Versionen aus dem Jahr 2010, deren Support jetzt endet. Zudem fanden wir ganze 13 verschiedene Versionen von Microsoft IIS für Webdienste sowie erstaunliche 89 verschiedene Versionen von Nginx, dem beliebtesten Webserver der Welt. Diese Anzahl unterschiedlicher Versionen ist höher als aus allen anderen regionalen Unternehmensgruppen, die wir bisher untersucht haben.

- **Der deutsche Automobilsektor sticht besonders hervor, was die Aufdeckung von Schwachstellen betrifft.** Während die VDP-Akzeptanz in der DB 314 weiterhin schleppend verläuft, da nur 34 Unternehmen irgendeinen Mechanismus zur Meldung von Schwachstellen in ihren Produkten oder der Infrastruktur aufweisen, ist die Automobilindustrie überdurchschnittlich beim Einsatz von VDP vertreten: 6 von 18 Automobilbetrieben verwenden ein VDP.

Vor dem Hintergrund dieser Erkenntnisse befasst sich der Rest des Berichts mit den fünf einzelnen, in der DB 314 bewerteten Cybersicherheitsbereichen.

Bevor Sie sich mit den Einzelheiten befassen, möchten wir darauf hinweisen, dass in Unternehmen, die von diesen Ereignissen betroffen waren oder es noch sind, häufig das Gefühl entsteht, dass ihre gesamte Zeit und Energie in die Bearbeitung von Notfällen geht, statt sich mit den ihnen zugrundeliegenden chronischen Problemen befassen zu können, die in diesem Bericht angesprochen werden. Unser Ziel ist es, Organisationen zu helfen, sicher und widerstandsfähig zu sein (und zu bleiben). Dazu haben wir einen spezifischen Anhang geschaffen, den Sie sich ggf. zuerst anschauen möchten, bevor Sie sich den einzelnen Abschnitten widmen.

E-Mail-Sicherheit in Unternehmen der Deutschen Börse 314

Wir alle kennen und lieben oder brauchen sie notgedrungen für unsere Tätigkeit: E-Mail. Sie ist ein Eckpfeiler der modernen Kommunikation, aber in den allermeisten Fällen auch sehr anfällig für bösartige Handlungen wie Spoofing oder Phishing.

Ein Kernthema von E-Mail ist die Authentizität der Quelle. In den letzten Jahren ist DMARC zum vorrangigen E-Mail-Validierungssystem geworden. DMARC erweitert die Grundlagen von zwei älteren E-Mail-Authentifizierungssystemen: Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM). Diese beiden prüfen die Autorisierung des Mail-Servers („Ist der Absender berechtigt?“) und die Unversehrtheit der E-Mail-Nachricht anhand von Schlüsselsignaturen („Wurde der Inhalt verändert?“). Die verschiedenen Komponenten von DMARC können dazu beitragen, direkte Bedrohungen zu mindern und potenzielle Reputationsschäden zu verhindern, die z. B. durch betrügerische E-Mail-Nachrichten zur Täuschung von Partnern, Lieferanten oder Kunden entstehen.

Ein richtig implementiertes DMARC-System kann unrechtmäßige E-Mails erkennen und bestimmen, was mit diesen E-Mails geschehen soll. DMARC kann für den Umgang mit suspekten E-Mail-Nachrichten auf einen unterschiedlichen Schweregrad konfiguriert werden, je nachdem wie streng IT-Administratoren vorgehen wollen. Die DMARC-Richtlinienoptionen umfassen:

- `None`, mit der verdächtige E-Mails an eine designierte E-Mail-Adresse gemeldet werden, die die DMARC-Benachrichtigungen überwacht.
- `Quarantine`, mit der verdächtige E-Mails in den Spam-Ordner geleitet werden und ein Bericht über ihren Empfang an die überwachende E-Mail-Adresse geht.
- `Reject`, mit der neben der Benachrichtigung an die überwachende E-Mail-Adresse die Übertragung der suspekten E-Mail-Nachricht ausbleibt.

Aufgrund seiner Wirksamkeit zur Unterbindung des Versands bösartiger Nachrichten per E-Mail betrachten wir DMARC als ein bedeutendes Risikominderungs-Tool und können die Implementierung nur empfehlen.

Obwohl die Vorteile von DMARC enorm sind, wurde es bisher leider nicht weitreichend genug implementiert.

Die Implementierungen von DMARC werden in den öffentlichen Einträgen des Domain Name System (DNS) verfolgt. Um zu erkennen, ob ein Unternehmen DMARC nutzt, muss lediglich der öffentliche DMARC-Eintrag der Organisation geprüft werden. Die Größe und die Arten der DMARC-Implementierungen entnehmen wir dem Vergleich der primären Domänen der DB 314-Organisationen mit den entsprechenden DMARC-Einträgen, die neben der DNS stehen.

Bitte beachten Sie, dass wir uns im Rahmen dieser Studie auf die Apex-Domänen der Organisationen konzentrieren und die anderen, im Besitz der Organisationen befindlichen Domänen außer acht lassen. Wir haben diesen Ansatz gewählt, weil die Art und Anzahl der eingerichteten Domänen in den Organisationen sehr unterschiedlich ausfällt. Durch den Fokus auf Apex-Domänen dienen sie uns als solider Indikator über die gesamte E-Mail-Sicherheitslage der Organisation. Wenn das Unternehmen noch nicht einmal in der Lage ist, DMARC in seiner primären Domäne zu installieren, kann man nicht unbedingt zuversichtlich sein, dass es in den weniger stark genutzten Domänen auf eindeutige E-Mail-Sicherheit achtet.

Diese veröffentlichten DMARC-Einträge sollen für jedermann zugänglich sein. Sie sind das Mittel, um festlegen zu können, wie E-Mails über DMARC validiert werden, wer über fehlgeschlagene E-Mail-Validierungen benachrichtigt werden soll und welche DMARC-Richtlinie bei der Verarbeitung ungültiger E-Mail-Nachrichten zum Einsatz kommt.

Ergebnisse

Auch wenn die Befragung nicht vollständig ist, stellten wir fest, dass 124 (oder etwa 39 %) der DB 314 Unternehmen in ihren primären Domänen mit DMARC arbeiteten, und dass diese Domänen alle richtig formatiert worden waren. Aus dem Satz der landesspezifischen Börsenindexe, die wir in der ICER-Reihe bisher untersucht haben, ist das vergleichsweise ein sehr niedriger Wert der DMARC-Verbreitung.

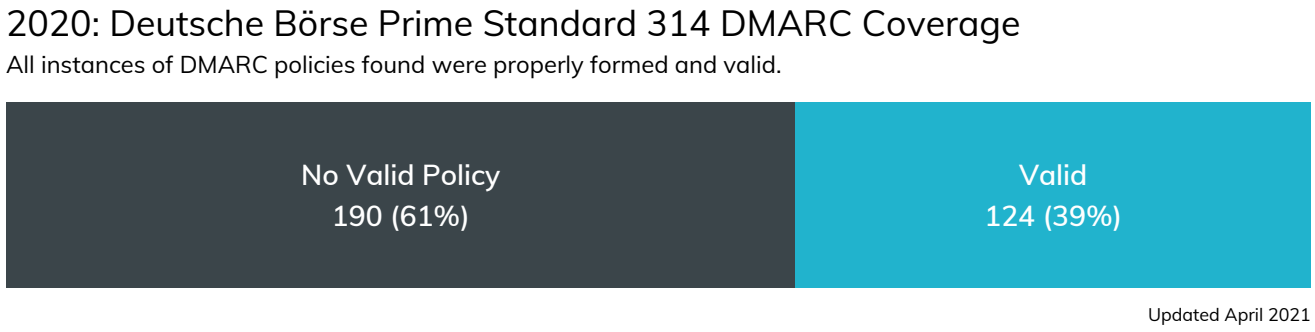


Abb. 1: 2020 Deutsche Börse Prime Standard 314 DMARC Coverage

Wenn wir die DMARC-Richtlinien noch etwas näher untersuchen, stellen wir fest, dass die am stärksten gültigen DMARC-Richtlinien auf "`none`" gesetzt sind, d. h. eine einfache Überwachung und Benachrichtigung, gefolgt von "`quarantine`", einer Richtlinie, die verdächtige E-Mails isoliert. Die am wenigsten genutzte Richtlinie ist "`reject`", der strengste Ansatz. .

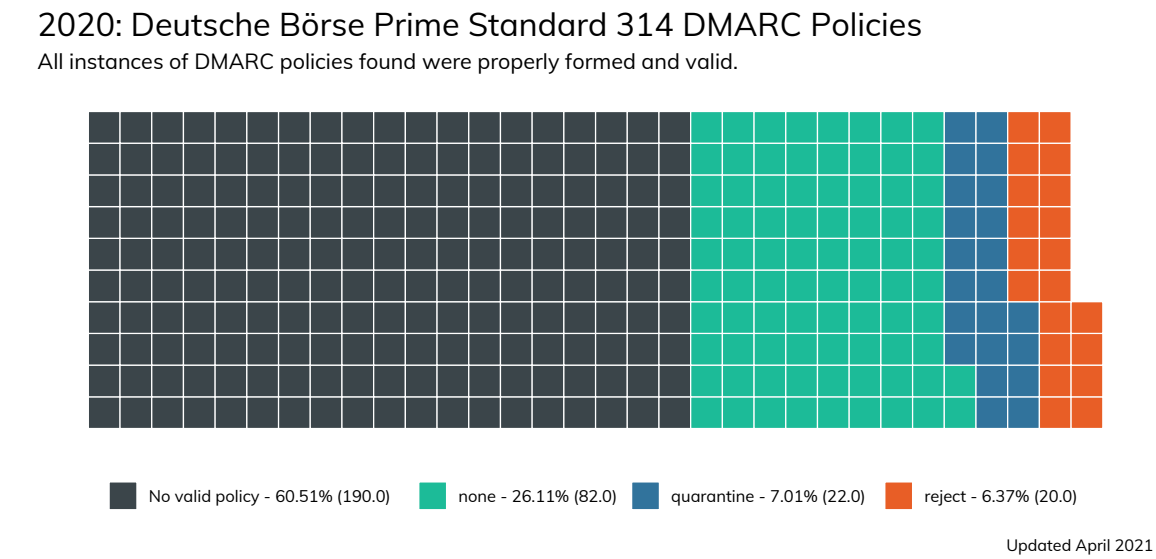


Abb. 2: 2020 Deutsche Börse Prime Standard 314 DMARC Polcies

Nach Branche

Wir können die Organisationen auch nach Branche trennen, um die DMARC-Unterschiede in den einzelnen Sektoren besser zu verstehen. Die am häufigsten genannten Branchen in der DB 314 sind u. a. die Fertigungsindustrie, Finanzdienstleistungen und Software.

Alarmierend ist dabei, dass in den meisten Branchen die Mehrheit der Organisationen einfach keine gültige Implementierung von DMARC-Richtlinien aufweist. Unzureichende oder gänzlich fehlende E-Mail-Sicherheitspraktiken sind in den Branchen weit verbreitet.

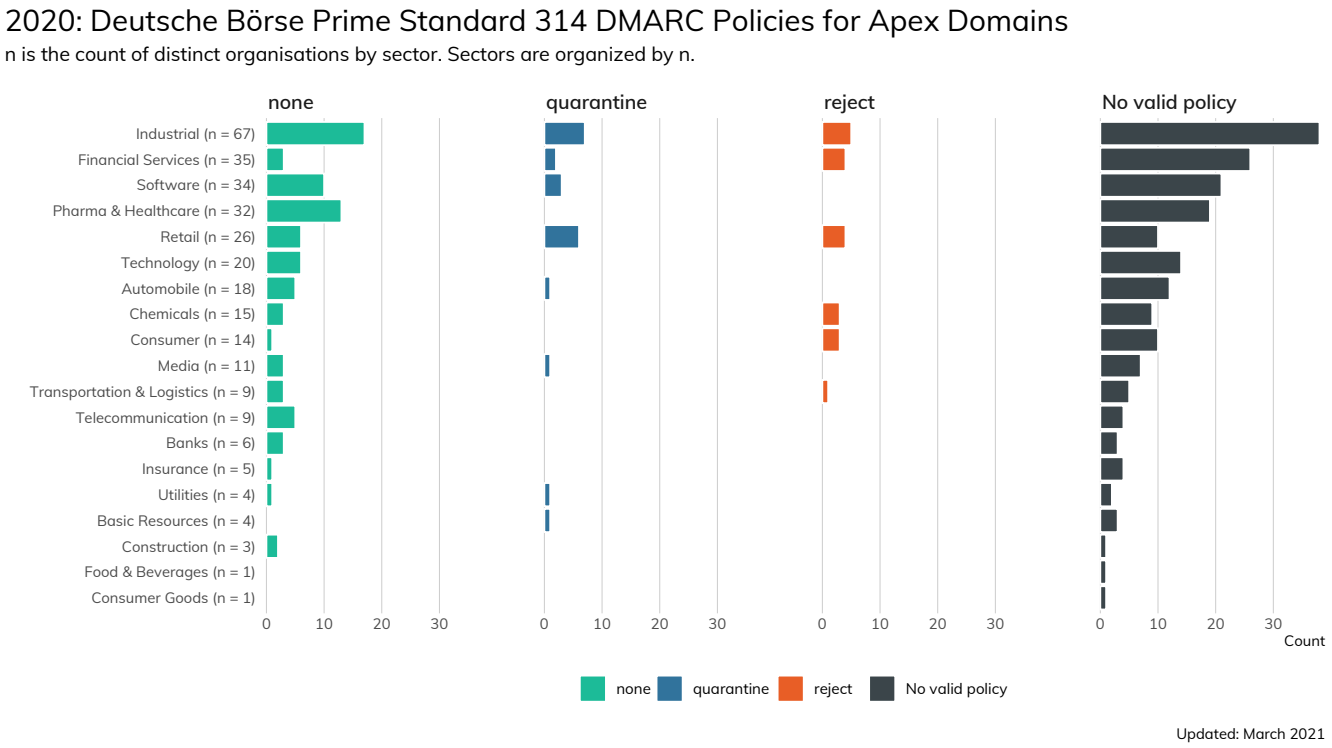


Abb. 3: 2020 Deutsche Börse Prime Standard 314 DMARC Policies for Apex Domains

Fazit für den CISO

Wenn DMARC in Ihrem Unternehmen noch nicht implementiert wurde, gehen Sie proaktiv vor, um es einzurichten.

Heutzutage kann man DMARC als einen Eckstein der E-Mail-Sicherheit sehen, denn es steht für das Engagement der Organisation, moderne IT-Sicherheitsnormen einzuhalten. Darüber hinaus ist ein Unternehmen ohne DMARC-Implementierung nicht in der Lage, schädliche E-Mail-Kampagnen zu erkennen und ihren Umfang, den Ursprung und Schweregrad zu analysieren.

Sobald die Entscheidung getroffen wurde, DMARC zu implementieren, ist es an der Zeit, die Anwendung der Richtlinien genauer ins Auge zu fassen. Die strenge `reject` Richtlinie ist sehr sicher, aber könnte dazu führen, dass rechtmäßige E-Mails gesperrt werden. Die etwas kulantere `quarantine` Richtlinie könnte ein Gleichgewicht zwischen der Problemverhinderung und einer gewissen Form von Behebung erzielen. Zumindest sollte irgendeine Form einer DMARC-Implementierung vorhanden sein, um unrechtmäßigen oder schlecht konfigurierten E-Mail-Datenverkehr zu überwachen.

Web-Dienst-Sicherheit bei den Deutsche Börse 314-Unternehmen

Ein Großteil aller Interaktionen einer Einzelperson mit IT erfolgt über irgendeine Form einer Webanwendung, aber was eine „Web-App“ ist, ist nicht immer eindeutig. Gleichermaßen weit gefasst sind die Sicherheitskontrollen zur Stärkung dieser Anwendungen. APIs, verteilte Authentifizierungsschemata, einseitige Anwendungen und statische Websites fallen in die allgemeine Kategorie der „Webanwendung“. Ohne zuvor die spezifische Anwendung zu benennen, lassen sich nur wenige Sicherheitsmaßnahmen finden, die für alle Webanwendungen gelten. Es gibt jedoch ein paar Maßnahmen, die wir hier behandeln werden.

Alle Webanwendungen sollten streng verschlüsselt werden, und für diese Regel gibt es nur sehr wenige Ausnahmen. Obwohl das vorrangig für Anwendungen gilt, die vertrauliche Informationen liefern, wie z. B. personenbezogene Informationen (PII), ist es auch dann wichtig, wenn Sie nur statische Informationen senden. Viele denken irrtümlicherweise, dass das einzige Risiko einer unsicheren Verbindung der Verlust der Vertraulichkeit sei, mit anderen Worten, dass die Informationen, nach denen jemand sucht, von einem betrügerischen Dritten gelesen werden könnten. Obwohl das sicher ein Risiko ist, wird häufig übersehen, dass durch den Mangel an Verschlüsselung die Verbindung manipulationsanfällig wird (Verlust der Unversehrtheit). Das bedeutet, betrügerische Dritte können nicht nur potenziell vertrauliche Informationen lesen, sondern sie könnten diese Informationen ändern oder ihren eigenen Inhalt injizieren, der Ihre Benutzer kompromittieren könnte.

Das Risiko einer bösartigen Content-Injektion besteht unabhängig davon, ob Ihre Webanwendung vertrauliche Informationen oder nur niedliche Bilder von Katzen übermittelt. Aufgrund dieses universellen Risikos für die Benutzer der Website und des Namens des Website-Betreibers empfehlen wir eine starke Verschlüsselung (in unserem Fall TLS) und die Durchsetzung seiner Verwendung über HTTP Strict Transport Security (HSTS). Für die Zwecke der hier behandelten Thematik sehen wir uns die primäre Domäne jedes Unternehmens an, da der Ruf eines Unternehmens zu allererst über die Domäne läuft.

HTTPS-Unterstützung

HTTPS ist das Protokoll, das sicherstellt, dass Web-Datenverkehr verschlüsselt und sicher ist. Es gibt einige Möglichkeiten, HTTPS in einer Umgebung zu konfigurieren.

- Nicht verfügbar (nur HTTP)
- Verfügbar und optional
- Erforderlich (HTTP „Strict Transport Security“ oder HSTS, konfiguriert)
- Erforderlich mit HSTS vorab geladen

Die Unterstützung von HTTPS durch Ihre Website ist eine Basisvoraussetzung für jede Internetpräsenz, und die Verschlüsselung steht an unmittelbar zweiter Stelle. HSTS vorab zu laden, ist technisch nicht ganz einfach, aber das sind Herausforderungen, die ein Web-Sicherheitsprogramm proaktiv in Angriff nehmen sollte.
Die DB 314 erlangt fast die perfekte Punktzahl, was die HTTPS-Akzeptanz angeht. Nur eine einzige Domäne unterstützt das sichere Protokoll nicht. HTTPS ist auch 2021 noch immer Pflichtprogramm in Bezug auf eine Internetpräsenz. Ein Versäumnis, sie zu übernehmen, reduziert auch Ihre Bewertung bei der Suchoptimierung (SEO), und daher hätten wir uns hier 100 % gewünscht.

HSTS-Akzeptanz

Die Aussichten für HSTS-Akzeptanz sehen leider sehr schlecht aus.

Wie Sie sehen, unterstützen nur rund 30 % der untersuchten Websites HSTS. Das ist wesentlich weniger, als wir aus anderen Berichten melden können. Wenn die Website HTTPS bereits vollständig unterstützt (diese Websites tun das alle), sollte es relativ einfach sein, HSTS zu implementieren, um sicherzustellen, dass Ihre Benutzer die sichere Version Ihrer Website besuchen. Die meisten dieser Websites stellen eine Umleitung von der unsicheren Version ihrer Homepage bereit – was jedoch keinen Man-in-the-Middle (MiTM) Angriff verhindern kann.

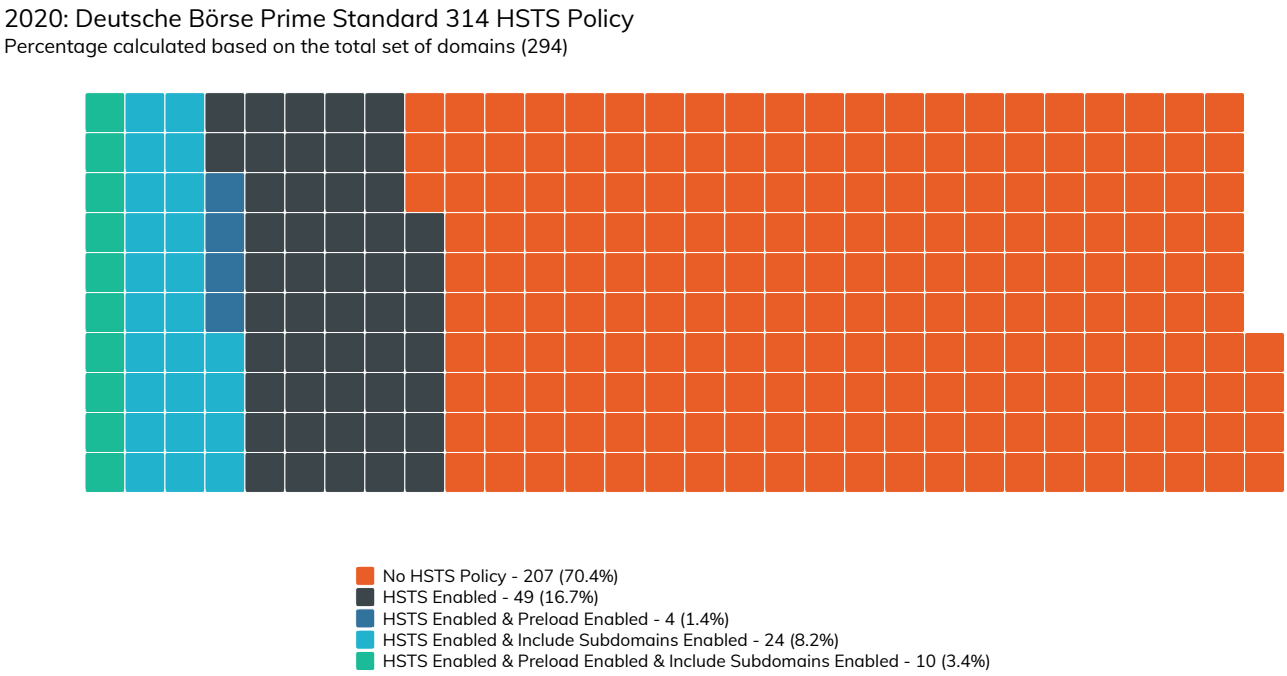


Abb. 4: 2020 Deutsche Börse Prime Standard 314 HSTS Policy

Keine der beobachteten Domänen hat HSTS manuell deaktiviert. Der Prozentsatz der Domänen mit dieser Konfiguration ist tendenziell niedrig, daher lässt sich diese Beobachtung wahrscheinlich auf die insgesamt geringe Anzahl der Domänen in dieser Liste zurückführen, die HSTS unterstützen.

39 % der Websites, die HSTS unterstützen, unterstützen auch die „`includeSubDomains`“ Anweisung, die die gesamte Domäne und alle Subdomänen schützt. Das ist eine fantastische Sicherheitsfunktion, aber in bestimmten Situationen kann eine Implementierung schwierig sein.

16 % der Websites mit HSTS unterstützen auch die „preload“ Anweisung. Diese Anweisung führt dazu, dass Crawler Ihre Website automatisch auf die globale Liste der bekannten Websites setzt, die HSTS unterstützen. Wenn ein unterstützender Browser auf eine Website mit aktiviertem vorab geladenen HSTS gelangt, garantiert dies, dass die erste Verbindung immer über HTTPS erfolgt, d. h. es beseitigt den einzigen Ort, an dem die Benutzer Ihrer Website für MiTM-Angriffe anfällig wären – die erste Verbindung mit Ihrer Website, bevor ein HSTS-Header erscheint. Diese Konfigurationsoption ist eine einfache Möglichkeit, eine zusätzliche Schutzebene

für Ihre Benutzer aufzubauen, und wenn Sie HSTS aktivieren, sollten Sie diese Option unbedingt hinzufügen. Obwohl es eine eher neuere Anweisung mit weniger Browser-Unterstützung ist, entsteht kein Nachteil, sie einzubeziehen (Browser, die HSTS nicht unterstützen, werden sie einfach ignorieren). Der Prozentsatz der Websites in der DB 314, die die preload-Anweisungen unterstützen, ist deutlich niedriger als in anderen Branchenberichten.

Zusammenfassung

Die Sicherung und Verschlüsselung von Datenverkehr auf Ihre benutzergerichteten Domänen ist nicht nur eine bewährte Vorgehensweise, sondern schützt auch den Ruf des Unternehmens. Die Sicherung von HTTP mit TLS war in den letzten Jahren ein wichtiger Schwerpunkt in der Web-Sicherheits-Community, und das aus gutem Grund. Fast alle DB 314-Unternehmen stellen eine sichere Version ihrer primären Website bereit, aber es gibt noch viel zu tun, bevor sie mit den bewährten Vorgehensweisen (Best Practices) mithalten können.

Die besonders schlechte Akzeptanz von HSTS in den DB 314 könnte ein Indikator sein, dass die Anwendungssicherheitsprogramme nicht mithalten können, insbesondere da andere, ausgeklügeltere Maßnahmen in ihrer Implementierung deutlich komplizierter sein können. Auch wenn die Standards sich schnell weiterentwickeln, ist es wichtig, auf dem Laufenden zu bleiben, wenn es darum geht, Ihren Markenwert zu schützen.

Fazit für den CISO

Wenn Sie sich schon länger keine Gedanken über die Verschlüsselung Ihrer Website gemacht haben, sollten Sie das jetzt tun. Der Ruf Ihres Unternehmens steht auf dem Spiel, wenn Webanwendungen mit Kundenausrichtung Sicherheitsverstöße erleiden. Berücksichtigen Sie diese Tatsache, wenn Sie Investitionsentscheidungen in verschiedene Sicherheitsprogramme vornehmen. Wenn die Website Ihres Unternehmens HSTS nicht unterstützt, wäre es vielleicht sinnvoll, herauszufinden, warum dem so ist. Ist es eine technische, organisatorische oder kostentechnische Beschränkung? Die Ursache benennen zu können, kann der passende Anlass zur Neubewertung Ihres gesamten Sicherheitsprogramms für Anwendungen sein.

Versionsunterschiede in den Unternehmen der Deutschen Börse 314

Für eine erfolgreiche Sicherheitslage in einer Organisation ist Komplexität der ultimative Widersacher. Die Vielfalt an Systemen, Technologien und Geschäftsprozessen stellt selbst die erfahrensten Sicherheitsteams täglich vor reale Herausforderungen, insbesondere wenn es um das Patch- und Schwachstellen-Management geht. In vielen Firmen kann das Patching von nur einer bedeutenden Schwachstelle eine Herkulesaufgabe sein. Vielfalt steigert zudem die Komplexität jeder weiteren Technologiekomponente. So kann ein Unternehmen beispielsweise unterschiedliche Webservertechnik verwenden. Jede Technologie kann wiederum selber unterschiedliche Versionen aufweisen, die sich direkt (negativ) auf die Konfigurationsverwaltung und das Patch-Management auswirken.

Um erkennen zu können, wie gut diese ausreichend ausgerüsteten Organisationen in diesem Bereich aufgestellt sind, haben wir uns drei Faktoren angesehen:

1. Die Vielfalt des Portfolios einer bestimmten Technologie – Webserver – die von jedem Unternehmen verwendet wird.
2. Wie gut dieses Portfolio instandgehalten wurde.
3. Wie gut die Organisationen geschäftskritische Dienste, wie E-Mail-Gateways, warteten.

Unsere Erkenntnisse zeigen:

- Innerhalb eines einzigen Technologie-Stacks (Webserver) haben Organisationen in einigen wichtigen Branchen – Finanzdienstleistungen, Medien, Pharma und Gesundheitswesen sowie Software – **zehn oder mehr verschiedene Versionen von Apache und/oder Nginx**. Zwölf Branchen haben mindestens einen Teilnehmer, der drei oder mehr verschiedene Versionen von IIS verwendet. Aufgrund der Komplexität der Tests und der Qualitätssicherung schafft diese Lage **größere Angriffsflächen** und macht es schwierig, Patches bereitzustellen (sofern Patches überhaupt zum Einsatz kommen).
- Unternehmen haben **große Schwierigkeiten, kritische IT-Infrastruktur** wie Microsoft Exchange **aktuell zu halten**. Nur rund 22 % (13 von 57) der Deutschen Börse 314, die immer noch mit Microsoft Exchange arbeiten und selbst hosten, führen aktuelle und unterstützte Versionen aus. Darüber hinaus führen 20 % nicht mehr unterstützte Versionen von Exchange 2010 aus, was sie für **die Ausnutzung zukünftiger Schwachstellen anfällig macht**.

Wir haben Project Sonar[5] und Recog[6] verwendet, um ins Internet gerichtete Technologien zu identifizieren, z. B. Webserver, Dateiserver, DNS, SSH usw. – die bei allen Unternehmen in den Deutschen Börse 314 verwendet wurden. Wir haben sie dann verfügbaren Common Platform Enumeration[7] (CPE)-Zeichenfolgen zugewiesen.

[5] https://www.rapid7.com/research/project-sonar
[6] https://github.com/rapid7/recog
[7] Definition und Datenbank von Common Platform Enumeration: https://nvd.nist.gov/products/cpe

Diese Methodik ist nicht allumfassend, da die Ergebnisse begrenzt werden durch:

- die Fingerabdrücke, die für Recog zur Verfügung stehen
- wie weitreichend jeder Fingerabdruckdienst ist (z. B. ob Recog Versionsinformationen extrahieren kann)
- die Ports und Protokolle, die Project Sonar untersucht
- unsere Messung von ausschließlich IPv4-Raum
- Sonar akzeptiert IPv4-Ausschlussanfragen (Opt-out)

Diese Einschränkungen führen in der Regel dazu, dass das Ausmaß der Erkenntnisse, wenn überhaupt, sogar unterschätzt wird.

Unterschiedliche Versionen bei den Webservern

Im Jahr 2018, als wir uns zum ersten Mal an die Analyse der Cyberexponierung der Deutschen Börse 314 heranwagten, haben wir den Begriff „Version Dispersion“ (unterschiedliche Versionen) geschaffen, um auf die Vielfalt der Versionen innerhalb einer Servicekomponente zu verweisen, die ein einzelnes Unternehmen im Internet exponierte.[8] Durch den dramatischen Anstieg der Unternehmensnutzung von Tools wie Kubernetes[9] haben wir eine Reduzierung der Anzahl unterschiedlicher Versionen der drei Webserver erwartet, d. h. IIS, Apache und Nginx, die wir zuvor erfasst haben.

Es gibt mindestens 69 verschiedene Versionen von Nginx[10], 51 verschiedene Versionen von Apache und 13 – ja, 13 – Versionen von IIS[11], die von den Mitgliedern der Deutsche Börse 314 betrieben werden. Schauen wir uns an, wie sich das auf die einzelnen Branchen verteilt.

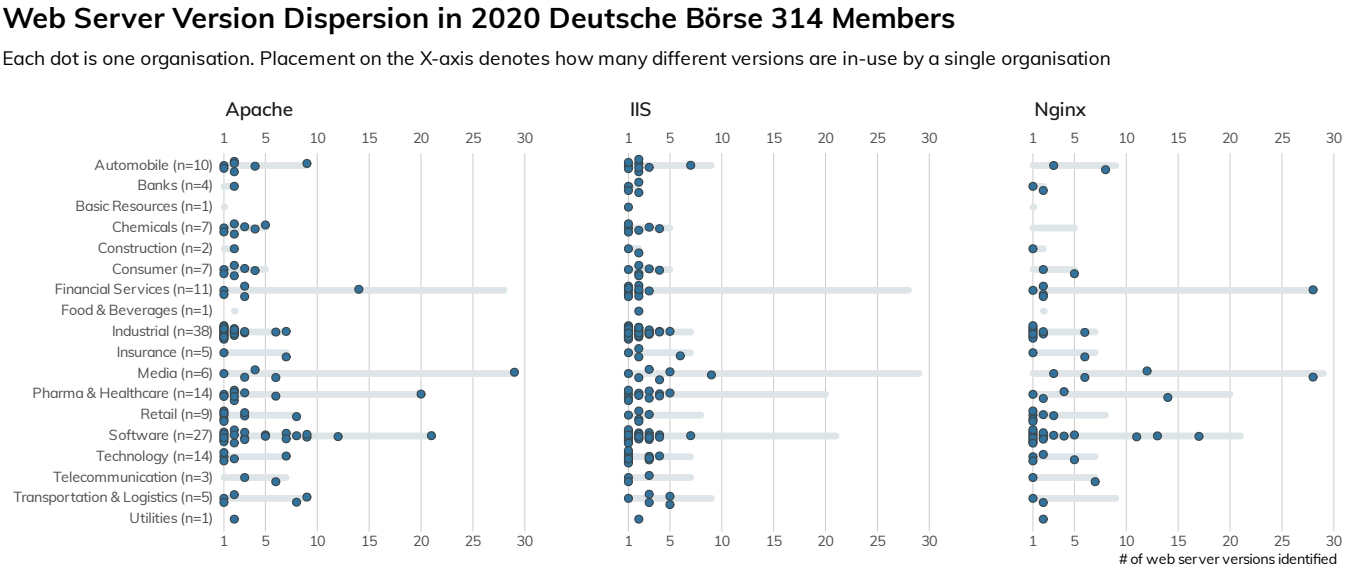


Abb. 5: Web Server Version Dispersion in 2020 Deutsche Börse 314 Members

[8] Eine Umfrage der Cloud Native Computing Foundation aus dem Jahr 2019 ergab, dass 78 % der Befragten Kubernetes in der Produktion einsetzen, was gegenüber 2018 mit 58 % ein enormer Zuwachs ist.

[9] Kubernetes Hauptseite: **https://kubernetes.io**

[10] Einige Unternehmen geben bekannt, dass sie einen bestimmten Server-Typ verwenden, bearbeiten aber die eindeutige Versionsnummer.

[11] Wir sehen häufig das Durchsickern von IIS-Build-Strings in angekündigten Server-Header-Bannern in IIS-Bereitstellungen.

Eine höhere Dichte von Punkten in Richtung „1“ auf der X-Achse zeigt an, dass jedes Unternehmen, das durch diese Punkte vertreten wird, eine geringere Anzahl von Versionen betreibt. Das bedeutet, dass sie mehr Kontrolle über ihre Server/Service-Bereitstellungen und -Konfigurationen haben, weniger Versionen verwenden, auf denen sie ihre Patches testen und Änderungen schneller und mit mehr Gewissheit als andere umsetzen können. Es bedeutet auch, dass sie strengere Regeln anwenden, nach dem Motto: „Sie müssen diese Größe haben, um einen Server im Internet bereitzustellen“, als Organisationen, die auf der X-Achse weiter rechts sind. Angreifer und Cyber-Versicherungsgutachter bemerken gleichermaßen diese Gegebenheiten und gehen mit höherer Wahrscheinlichkeit gegen Organisationen vor, die sich verstärkt wie im „wilden Westen“ präsentieren.

Zwischen den verschiedenen Webserver-Versionen in den Unternehmen der Deutschen Börse 314 und denen, die wir aus den FTSE 350 und Fortune 500 ICERs beobachtet haben, zeichnet sich ein bemerkenswerter Unterschied ab. Ein Grund dafür ist, dass an der Deutschen Börse notierte Unternehmen anscheinend eine Vorliebe für „die Cloud“ haben, um möglicherweise eine schnellere globale Konnektivität mit den Informationen oder Diensten der Web-Services zu haben, die sie nutzen. Wir messen in den ICERs keine „Cloud“-Ressourcen, von daher sind diese positiven Ergebnisse unter Berücksichtigung dieses Aspekts zu sehen.

Unterschiedliche Version: Schwerpunkt Microsoft Exchange

Einige ins Internet gerichtete Dienste haben eine höhere Bedeutung als andere. Einerseits kann man natürlich einen schwerfälligen alten Apache HTTPD-Server mit dem Internet verbinden, dessen einzige Schwäche möglicherweise eine Anfälligkeit für Denial-of-Service ist. Es ist jedoch etwas völlig anderes, alte Versionen von Infrastruktur auszuführen, die die meisten Unternehmen als geschäftskritisch ansehen würden (und es auch sollten), wie Microsoft Exchange-Server oder VPN/Gateway/Remote Access Services.

Für einen Einblick, wie diese Unternehmen geschäftskritische Dienste instandhalten, haben wir uns die Verfahren zu Microsoft Exchange angesehen. Im Gegensatz zu ihren Fortune 500 Kollegen haben nur 18 % der Unternehmen der Deutschen Börse 314 immer noch mindestens 1 Exchange-Server mit Internetverbindung, der geschäftskritische E-Mail bearbeitet. Im Laufe der Zeit hat sich herausgestellt, dass Exchange eine ganze Reihe von Schwachstellen mit unterschiedlichem Schweregrad aufweist:

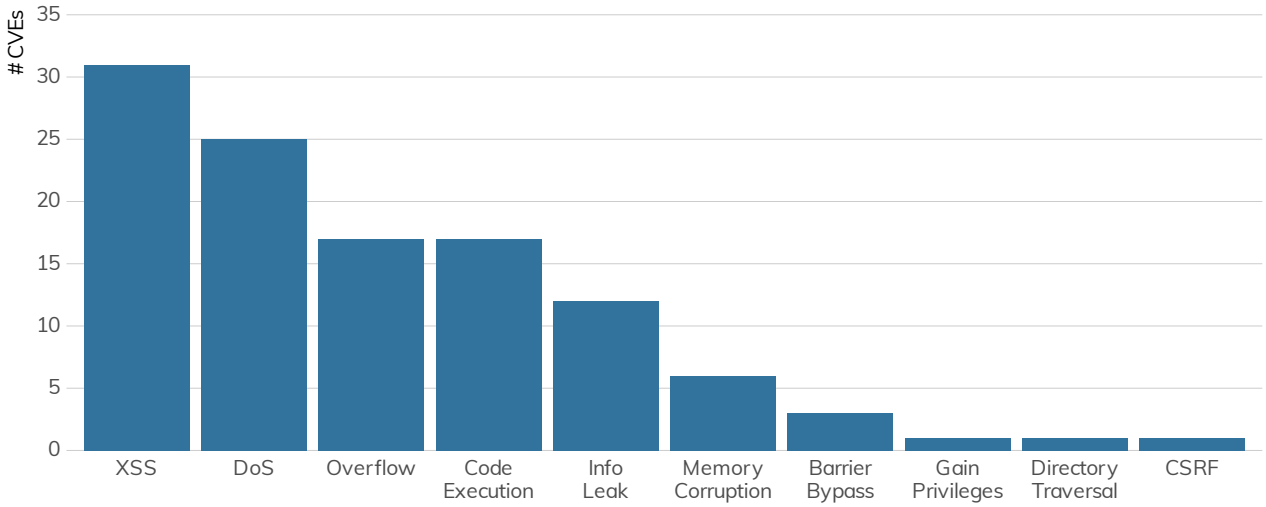


Abb. 6: Exchange CVEs by Type

[12] Die Verbreitung von Microsoft 365/Office 365 nimmt generell stetig zu, wobei 70 % der Fortune 500-Unternehmen einen oder mehrere Dienste, einschließlich gehostetem Exchange, nutzen. Quelle: https://www.thexyz.com/blog/microsoft-office-365-usage-statistics/

Dieser niedrigere Prozentsatz (im Vergleich zu den Fortune 500) ist unter dem Vorbehalt zu sehen, dass viele der Unternehmen, die regelmäßig in die Liste der Deutsche Börse 314 aufgenommen werden, Holding-Unternehmen oder Meta-Körperschaften sind, die wenig Infrastruktur haben und perfekte Kandidaten für Cloud-Hosted E-Mail-Dienste sind. Allerdings haben sich 57 Organisationen (mit Ausnahme von 3 ISPs, die allgemeines Service-Hosting zulassen) für den Alleingang entschieden. Man sollte davon ausgehen können, dass sie sich der Gefahren eines selbst gehosteten Exchange-Servers bewusst sind und sich darum kümmern, dass dieser wichtige Dienst optimal resilient ist, zumindest was Sicherheits-Patches angeht. Sehen Sie das auch so?

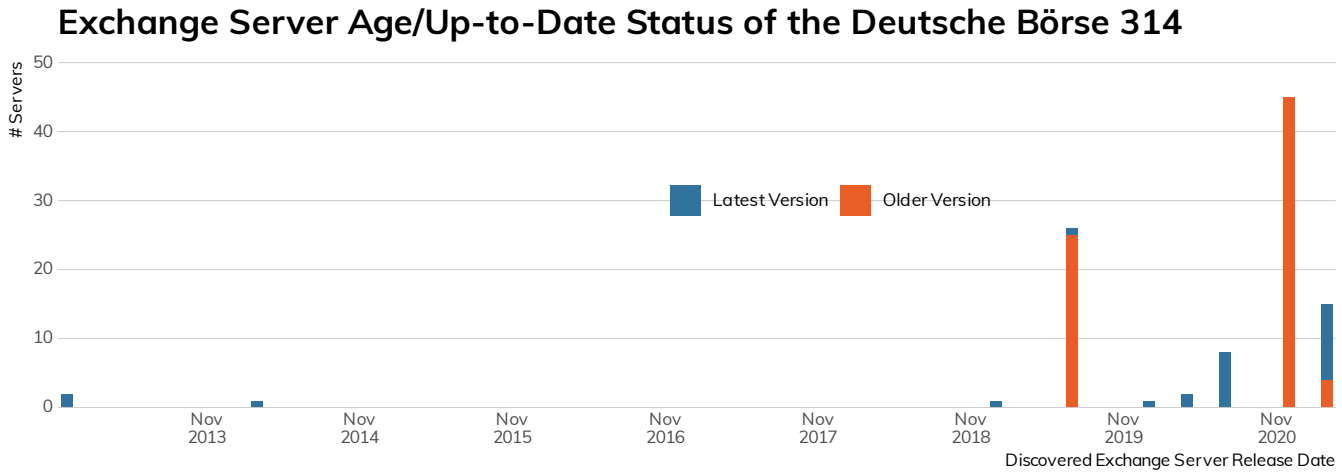


Abb. 7: Exchange Server Age/Up-to-date Status of the Deutsche Börse 314

Die oben stehende Abbildung zeichnet ein ziemlich beunruhigendes Bild über den Zustand von Microsoft Exchange in Unternehmen der Deutschen Börse 314, was sowohl die Aktualität (z. B. das Alter einiger Serverversionen) als auch den Support der implementierten Version im Rahmen einer[13] standardmäßigen Microsoft Support-Vereinbarung[14] betrifft. Positiv zu bewerten ist, dass 69 % der erkannten, mit genauen Versionsangaben festgehaltenen Instanzen das Release von 2020/2021 waren.

Glücklicherweise lief auf keinem Server Exchange 2007 (das schon länger eingestellt ist). Leider haben eine Handvoll der Deutschen Börse 314 die Benachrichtigung im Oktober 2020 zur Produkteinstellung[15] von Exchange 2010 offenbar nicht wahrgenommen.

[13] https://docs.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates

[14] Wir verwenden den Begriff „nicht unterstützt“ als Universalbegriff für „nicht in der neuesten Version“ sowie für eine Version, deren Support beendet wurde. Beachten Sie, dass dabei nicht berücksichtigt wurde, ob ein Unternehmen eine angepasste oder erweiterte Supportvereinbarung mit Microsoft unterhält, obwohl das für die Ausnutzung von Schwachstellen kaum eine Rolle spielt.

[15] https://docs.microsoft.com/en-us/microsoft-365/enterprise/exchange-2010-end-of-support?view=o365-worldwide

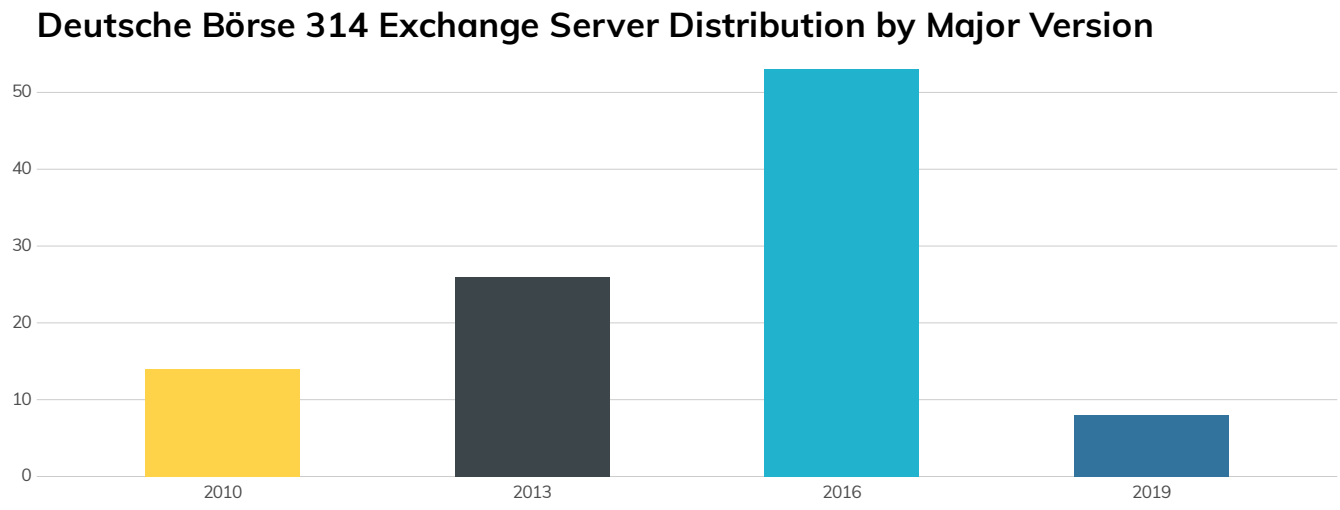


Abb. 8: Deutsche Börse Exchange Server Distribution by Major Version

Sollte Ihr Unternehmen Probleme haben, mit den Exchange Patches Schritt halten zu können, haben Sie noch etwas Spielraum, um sich herauszureden. Microsoft zögert nicht, weiterhin eine große Menge an laufenden Aktualisierungen der moderneren Versionen von Exchange herauszugeben:

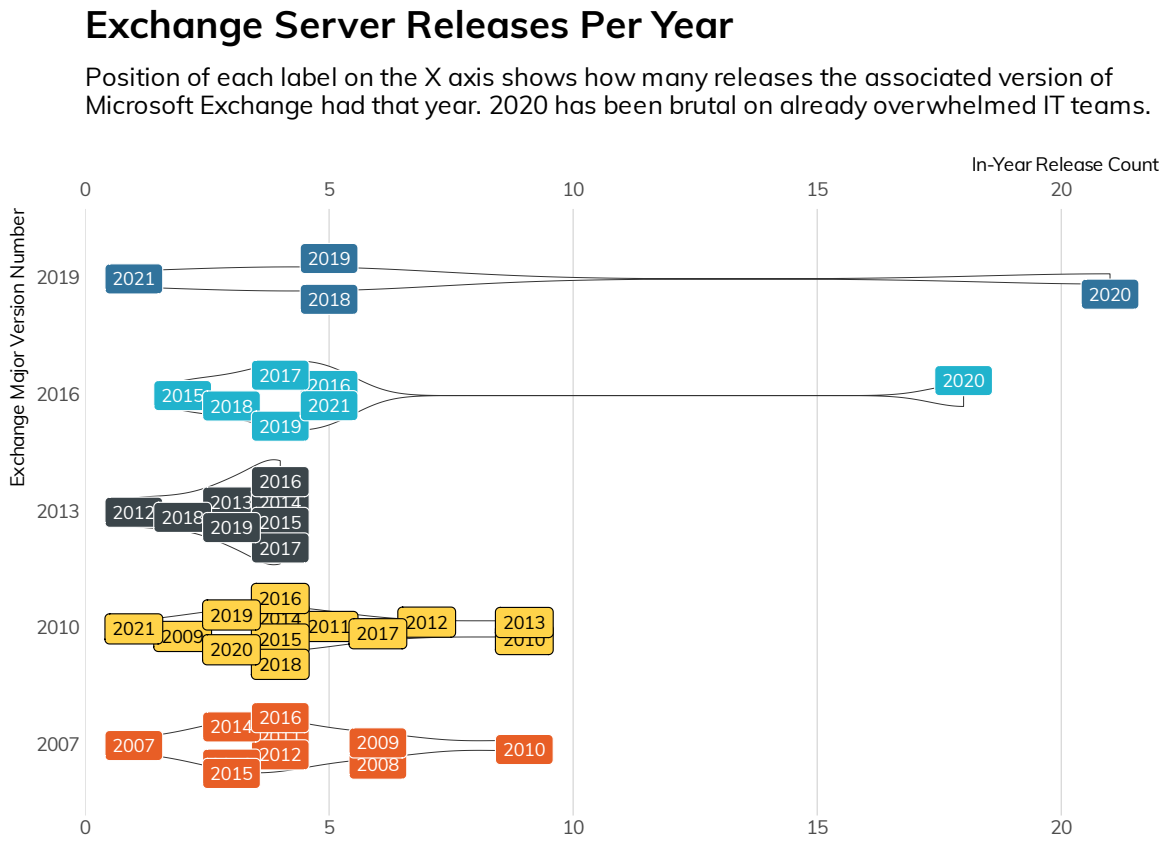


Abb. 9: Exchange Server Releases Per Year

Die Aussichten sind branchenübergreifend unverändert trüb.[16] Abbildung 11 zeigt das Release und den aktuellen Status von Exchange in allen Branchen mit Exchange-Servern an, und praktisch alle haben Probleme, auf dem neuesten Stand zu sein.

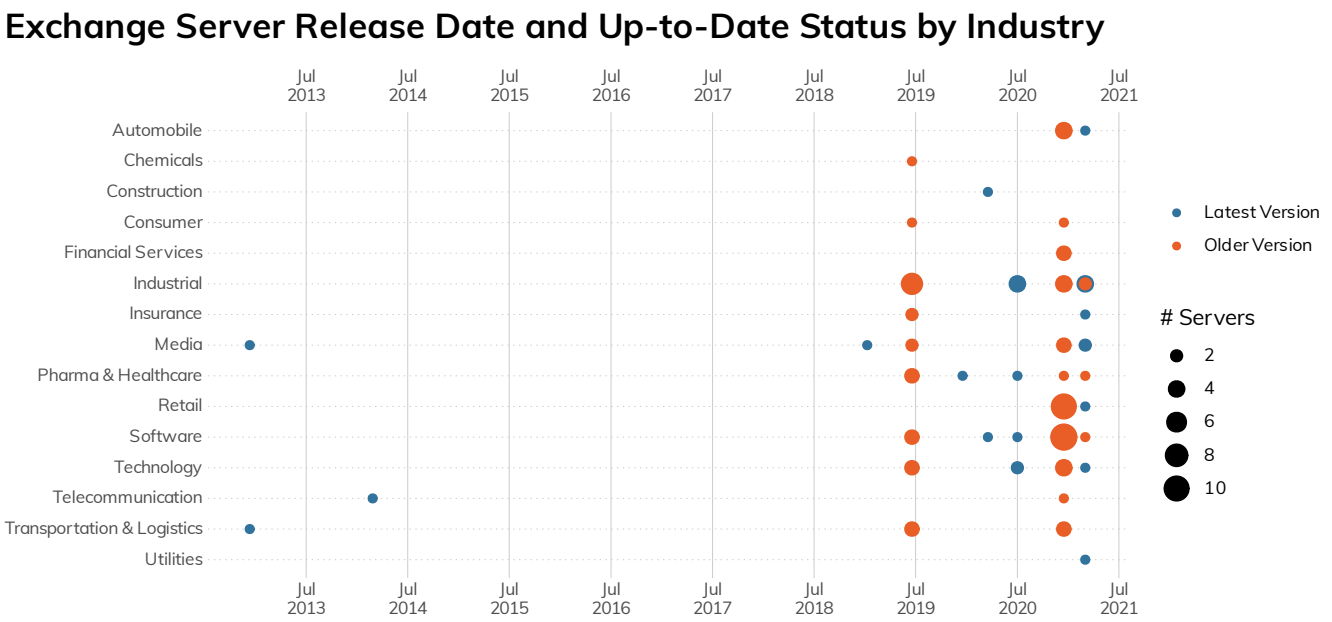


Abb. 10: Exchange Server Release Date and Up-to-Date Status by Industry

Wenn es problematisch ist, die Exchange-Implementierung aktualisiert, sicher und resilient zu halten, können Sie bis zu einem gewissen Grad beruhigt sein, denn selbst Microsoft hat Probleme bei der Normalisierung von gehosteten Exchange (Microsoft 365) Build-Ebenen. Dieses Diagramm ist bei Weitem nicht so erschreckend wie die Momentaufnahme aus dem Dezember 2020 von den Fortune 500 ICER, deren aktuellste Bereitstellungen im mittleren Bereich feststeckten, und eine fast gleiche Anzahl unterschiedlichster Versionen am Netzwerkrand des Internet kursierten.

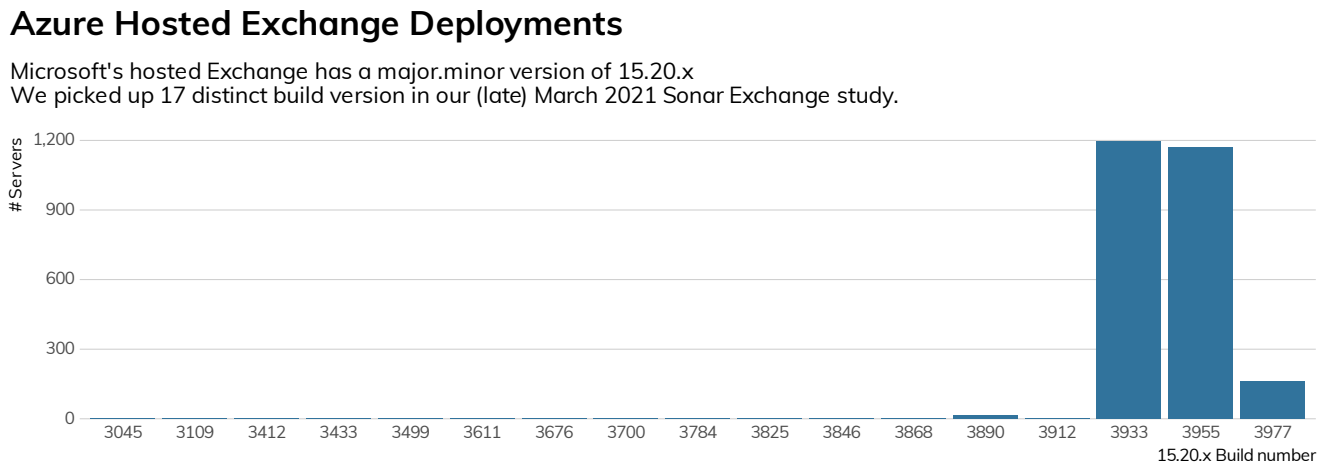


Abb. 11: Azure Hosted Exchange Deployments

[16] Yes, we took the obvious pun.

Fazit für den CISO

In diesem Kapitel sprechen wir mit zwei verschiedenen CISO-Vertretern: denen, die sich in den einzelnen Abschnitten wiedererkennen, und jenen, die mit vergleichbaren Organisationen als Geschäftspartner oder Lieferanten zusammenarbeiten.

Wenn Sie ein Sicherheitsleiter sind, der Resilienz und Sicherheit in die DNA seines Unternehmens einbauen möchte, sind Anliegen wie Technologisierung, Versionskontrolle und die Wartung geschäftskritischer Dienste unumgänglich und nicht verhandelbar. Die guten Nachrichten sind, dass dies nicht nur „Sicherheitsfragen" sind. Unternehmen stellen Dienste bereit, um einen geschäftlichen Bedarf zu erfüllen. Es ist erheblich einfacher, die Betriebszeit und Stabilität aufrechtzuerhalten, wenn weniger bewegliche Teile gewartet werden müssen. Um den Einstieg der Kollegen zu gewährleisten, erfassen Sie historische und aktuelle Daten über den Serviceverfall (und/oder Ausfälle). Setzen Sie hinzu, wie viel Zeit IT-, Anwendungs- und Betriebsteams mit dem Support der Komponenten der einzelnen Geschäftsprozesse verbringen. Wenn Sie diese Informationen in Beziehung setzen zum Aufkommen und den Schweregraden identifizierter Schwachstellen (CVE-basierend oder anderweitig), finden Sie Bereiche mit einem soliden Geschäftsfall, der die Zusammenarbeit zwecks Verbesserung plausibel macht. Sobald sich Verbesserungen in den einzelnen Bereichen bemerkbar machen, sind Sie in einer besseren Lage, Veränderungen auch in anderen Bereichen anzustoßen.

Alle, die beunruhigende Fakten in diesem Abschnitt befürchteten, sollten bei der Bewertung Dritter im Auftrag der Personen mit Zuständigkeit für die Geschäftsprozesse in Ihrem Unternehmen diese Bereiche im Auge behalten. Es sollte nicht schwerfallen, bei der Befragung zu den potenziellen Schwachstellen[17] auch zu prüfen, ob die erhaltenen Antworten stimmen. Es kann nicht garantiert werden, dass die interne Exponierung in Unternehmen dem entspricht, was extern sichtbar ist. In der Regel ist es jedoch sehr viel wahrscheinlicher, dass das interne Bild viel schlimmer ist, als was der Außenwelt präsentiert wird. Von den Partnern und Lieferanten ein höheres Niveau an Sicherheit und Resilienz zu verlangen, mindert nicht nur das Risiko für Ihr Unternehmen, sondern hat auch weitreichende positive Auswirkungen auf andere Unternehmen, die Ihrem Vorbild folgen wollen.

[17] Und obendrein umsonst! https://opendata.rapid7.com/

Riskante Services in Unternehmen der Deutschen Börse 314

Einige Serviceleistungen werden generell als riskant eingestuft, wenn sie im öffentlichen Internet verfügbar sind. So ist es z. B., abgesehen von sehr wenigen Ausnahmen[18], nicht ratsam, SMB-Dateifreigaben ins Internet zu setzen. Dabei können Daten exponiert, Umgebungsinformationen wie Domänennamen bekanntgegeben, Brute-Force-Angriffe gegen Zugangsdaten verübt und ein Vektor geschaffen werden, der die Schwachstellen in der Implementierung von Windows Server Message Block (SMB) ausnutzt, wie wir bei den Conficker[19] und WannaCry[20] Würmern gesehen haben.

Bei unserer Untersuchung im öffentlichen Internet ist uns bewusst geworden, dass wir nur die Oberfläche von Informationen sehen. Oft versuchen wir Wege zu finden, um zu verstehen, was diese Informationen uns über die Organisationen mitteilen, die diese Dienste betreiben. Wir können uns Konfigurations- und Protokolldetails ansehen und sie als Proxy-Markierungen für die interne Umgebung und die Ausgereiftheit der Sicherheit eines Unternehmens einsetzen.

Wenn wir z. B. einen SMB-Dienst entdecken und erkennen können, dass er den[21] mit Windows Vista[22] und Server 2008 eingeführten SMBv2 nicht unterstützt, können wir daraus Schlüsse über das Alter des Betriebssystems und/oder die Anforderungen in Bezug auf Legacy-Kompatibilität ziehen.

Wenn ein Unternehmen Telnet[23]-Verbindungen mit Routern in einem anderen Land ermöglicht, können wir daraus Schlüsse über das Alter der Geräte und die Sicherheitsrichtlinien für sichere Protokolle und Access-Control-Listen (ACLs) im Netzwerk ziehen.

Um einen Eindruck zu gewinnen, wie gut die DB 314 Unternehmen in diesem Bereich aufgestellt waren, haben wir uns SMB, Windows Remote Desktop Protocol (RDP) und Telnet über die Standard-Ports in ihrem öffentlichen IPv4-Adressenraum angesehen und sofern vorhanden die Servicedaten überprüft.

Unsere Erkenntnisse zeigen:

- Am meisten exponiert war die pharmazeutische Industrie und das Gesundheitswesen, wobei ein besonders hohes Auftreten im Umfeld eines Unternehmens auffällt.
- Unter den Hosts, die SMB exponierten, gaben alle den SMB-Hostnamen, den DNS-Namen und den Fully Qualified Domain Name (FQDN) preis, der auf dem Host konfiguriert ist.
- In 19 Unternehmen wurden 101 RDP-Dienste gefunden. Diese konzentrierten sich aufgrund der übergroßen Präsenz eines Unternehmens stark in der Pharmabranche- und im Gesundheitswesen.

Wir haben Project Sonar und Recog verwendet, um ins Internet gerichtete SMB-, Windows Remote Desktop Protocol (RDP)-[24] und Telnet-Dienste auf den Standard-Ports zu identifizieren, die jedes Unternehmen in den DB 314

[18] https://docs.microsoft.com/en-us/sysinternals/
[19] https://de.wikipedia.org/wiki/Conficker
[20] https://de.wikipedia.org/wiki/WannaCry
[21] https://wiki.wireshark.org/SMB2
[22] Der mittlerweile alt genug ist, um in den meisten US-Bundesstaaten den Führerschein zu machen (entstanden: November 2006)
[23] https://de.wikipedia.org/wiki/Telnet
[24] https://de.wikipedia.org/wiki/Remote_Desktop_Protocol

einsetzte. In jedem Fall haben wir das Protokoll voll ausgehandelt, um zu verifizieren, dass wir tatsächlich mit dem erwarteten Dienst kommunizierten. Diese Vorgehensweise kann nicht alles erfassen, da die Ergebnisse durch diese Gegebenheiten beschränkt werden:

- Die Dienste werden nur auf den Standard-Ports beobachtet. Telnet und auch RDP, wenn auch weniger häufig, können auf nicht-standardmäßige Ports verlegt werden.
- Die Messungen werden nur im IPv4-Raum durchgeführt.
- Bestimmte IP-Bereiche werden von Sonar auf Anfrage nicht untersucht.
- Bestimmte die Cloud und ISP betreffende Bereiche wurden ausgeschlossen. Die Auswirkungen sind je nach Unternehmen sehr unterschiedlich.
- Bestimmte Netzwerke wurden ausgeschlossen, wenn sie unseres Erachtens nach Kunden zugewiesen waren oder anderweitig Dritten zugeordnet werden können.

Unter anderweitig gleichen Bedingungen ergeben diese Beschränkungen in der Regel, dass nicht alle Vorkommnisse erfasst oder gemeldet werden.

Erkenntnisse: RDP, SMB und Telnet

Gleich zu Beginn dieses Abschnitts soll daher die Aussage stehen, dass **alle Werte über Null dieser im allgemeinen Internet offengelegten Dienste** in Organisationen mit einem ausgereiften Sicherheitsprogramm inakzeptabel sind. Die Follower des Rapid7-Blogs und der bisherigen Rapid7-Forschungsberichte sind mit diesem Rat sehr vertraut. Aber mit Blick auf den Kalender 2021 müssen wir feststellen, dass es schon eine Weile her ist, seit der letzte große Wurm-Angriff im Internet stattgefunden hat. NotPetya (SMB) war 2018, WannaCry (auch SMB) war 2017 und Mirai (Telnet) liegt noch weiter zurück: 2016. Trotz aller Schwachstellen und der Ausbeute, die wir 2019 und 2020 erlebt haben, sind wir scheinbar überfällig für einen weiteren selbstreplizierenden Angriff über offene Ports auf unsichere Dienste. Wenn Sie Ihre Exponierung dieser Dienste beenden, können Sie mit Sicherheit Zeit für die spätere Bereinigung sparen.

Windows Remote Desktop Protocol (RDP)

Während einige davon ausgehen, dass RDP als Ausnahme dieser Regel gelten sollte, sind wir der Meinung, dass es weitläufig verfügbare Verfahren und Technologien wie virtuelle private Netzwerke (VPNs), RDP-Gateway-Dienste und Access-Control-Listen (ACLs) für die Firewall gibt, die das aus dieser Technologie entstehende Risiko beseitigen. Als allgemein gültige Regel gilt: **RDP darf nicht Quellenadressen außerhalb des Unternehmens ausgesetzt werden**.

Da wir schon beim Thema RDP sind, wollen wir gleich die Ergebnisse besprechen. Über den Standard-RDP-Port 3389/TCP liefen bei 19 Unternehmen 101 Dienste. Ein Unternehmen aus der Pharma- und Gesundheitsversorgungsbranche beanspruchte 45 % der beobachteten RDP-Dienste.

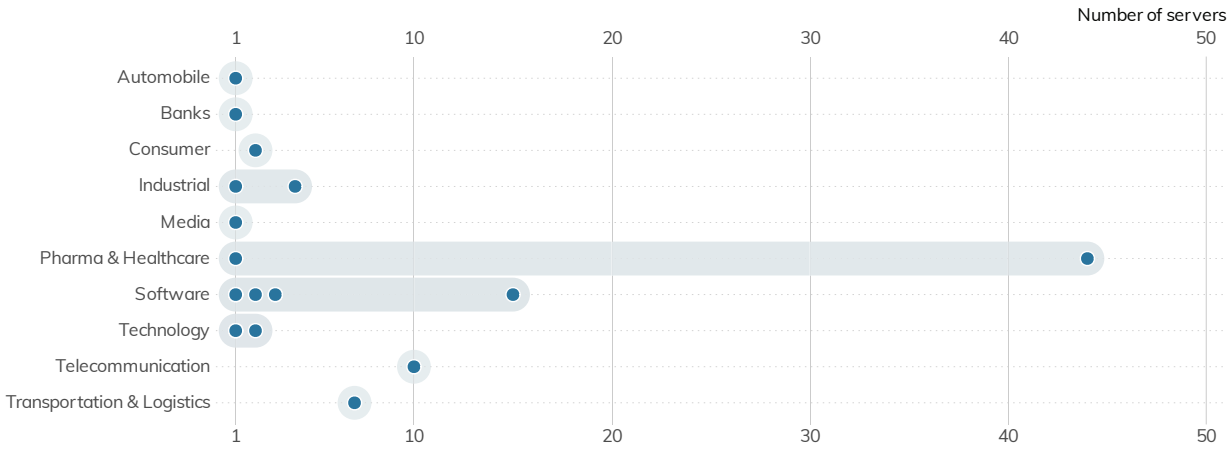


Abb. 12: Port 3389 Distribution by Industry

Die oben stehende Grafik zeigt, dass die Zahlen in der Mehrheit nur wenigen Unternehmen zuzuordnen sind, aber es sind einige Branchen vertreten.

Gut zu bewerten ist die Tatsache, dass in Hinblick auf die Sicherheitsanforderungen für RDP-Authentifizierung 91 % der Unternehmen Network-Level-Authentifizierung (NLA) einsetzten.[25] NLA, die mit Windows Server 2008 eingeführt wurde, ermöglicht den Transport Layer Security (TLS)-Schutz von Daten während des Transports. Zudem stärkt sie die Authentifizierungsoptionen und verringert erheblich die Risiken und Auswirkungen von Brute-Force- und bestimmten Denial-of-Service-Angriffen. Seit Windows 2012 ist NLA standardmäßig aktiviert. Ein Mangel an NLA ist quasi ein Hinweis auf eine ältere Infrastruktur und zwar entweder auf dem eigentlichen Server oder als Kompatibilitätsvoraussetzung für ältere Clients. Der einzige andere Grund, weshalb NLA nicht aktiviert wurde, ist der, dass es die Authentifizierung mit abgelaufenen Passwörtern verhindert. Genau das ist ein weiterer Grund, weshalb RDP Gateway-Server, VPN oder andere Infrastruktur installiert werden sollte, damit es möglich wird, das Passwort zu ändern und auch den sicheren Zugriff auf Remote-Desktop-Dienste zu aktivieren.

Windows Server Message Block (SMB)

Das SMB-Protokoll dient der Datei- und Druckfreigabe sowie der prozessübergreifenden Kommunikation unter Windows mit kompatiblen Netzwerken. **Wir weisen in jedem Bericht darauf hin,[26] aber SMB sollte niemals im Internet exponiert werden.** Zu den Risiken gehören Datenlecks aus Dateifreigaben, kompromittierte Zugangsdaten aufgrund von Brute-Force-Angriffen und Malware-Infektionen (denken Sie dabei nur an die bereits erwähnten Conficker und WannaCry) aufgrund von Schwachstellen im Host-Betriebssystem oder im Service. Angesichts der vielfältigen Optionen zur sicheren Dateifreigabe ist eine Freigabe über SMB das Risiko nicht wert.

[25] https://en.wikipedia.org/wiki/Network_Level_Authentication
[26] https://www.rapid7.com/research/report/nicer-2020/#smb-tcp-445

Bei der Befragung der DB 314 haben wir uns entschieden, zwei verschiedene SMB-Ports ins Auge zu fassen: 139/TCP und 445/TCP Port 139/TCP wird für ältere Varianten von SMB verwendet. In der Regel ist das ein Anzeichen dafür, dass sehr alte Software und veraltete Anforderungen bestehen. In unseren Befragungen trafen wir auf 9 Server in drei Unternehmen. Alle führten einen Open-Source-SMB-Server namens Samba aus.[27] Die älteste Version von Samba (3.0.36), die wir fanden, kam Ende 2009 heraus und enthält eine ganz Reihe kritischer Schwachstellen.

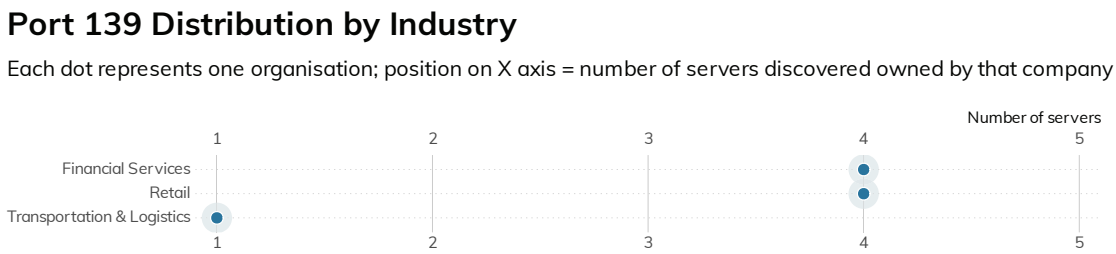


Abb. 13: Port 139 Distribution by Industry

Auch haben wir SMB auf Port 445/TCP untersucht. Das mit Windows 2000 eingeführte Transportmodell für SMB beseitigte einige der Altlasten des vorhandenen Protokolls. Wir fanden in unserer Untersuchung 40 Server in 15 Organisationen

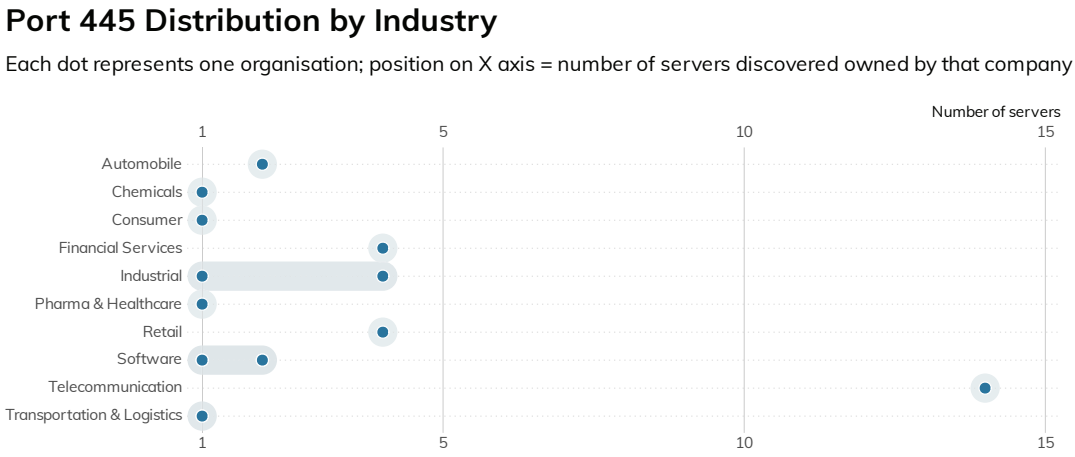


Abb. 14: Port 3389 Distribution by Industry

[27] https://www.samba.org/

Die Tatsache, dass diese SMB-Server im Internet vorhanden sind, ist ein Anlass zur Sorge, aber als wir uns die Protokollkonfigurationen näher ansahen, nahm unsere Sorge nur zu. Alle Server unterstützten SMBv1, d. h. ihnen fehlen mehrere kritische Sicherheitskontrollen. Angreifer können Clients zwingen, von sichereren Versionen des Protokolls auf SMBv1 herunterzurüsten. Alle 40 Server, die wir beobachtet haben, unterstützten eine neuere Version von SMB und hätten demnach, ausgenommen einer Abhängigkeit von veralteten Systemen, keinen Bedarf, SMBv1 zu aktivieren. Wir schließen uns daher explizit der Aufforderung seitens Microsoft an, SMBv1 zu deaktivieren.[28]

SMBv3 wurde mit Windows Server 2012 herausgegeben und beinhaltete viele Sicherheits- und Leistungsverbesserungen, wie[29] z. B. die Verschlüsselung der Daten mit Wire-and-Protocol-Herabstufungsschutz. SMBv3 wurde auf 68 % der untersuchten Server unterstützt.

Diese SMB-Dienste gaben auch Informationen über das Unternehmen frei. Alle Dienste stellten einen Hostnamen, einen DNS-Namen und einen vollständig qualifizierten Domänennamen (FQDN) bereit, der auf dem Host konfiguriert wurde. Diese Informationen können auf die Rolle (VCENTER01) oder auf die interne Organisationsstruktur `(db1.prod.us.corp.local)`hinweisen.

Telnet

Telnet ist ein textbasiertes Protokoll, das zum Remote-Zugriff auf Geräte verwendet wird. Es überträgt fast immer die Zugangsdaten und Daten in Klartext und bietet keinen Schutz gegen Man-in-the-Middle (MiTM)-Injektion von Befehlen oder Daten. Das ursprünglich 1969 entwickelte Telnet hat sein „Verfallsdatum“ längst überschritten und wurde durch andere, viel sicherere Technologien wie SSH ersetzt. Bei unserer Untersuchung stießen wir auf 70 Hosts in 19 Unternehmen. Die Mehrheit dieser Hosts befindet sich im Pharmasektor und im Gesundheitswesen.

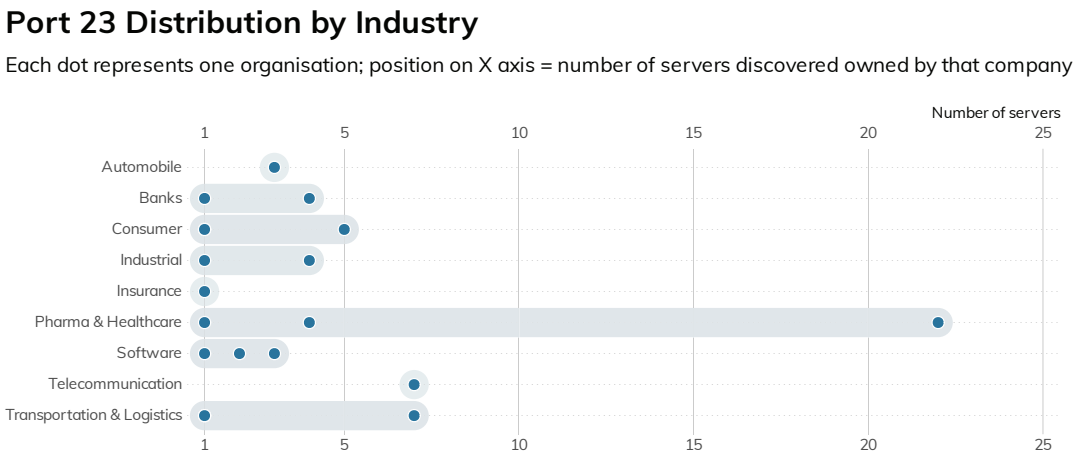


Abb. 15: Port 23 Distribution by Industry

[28] https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858
[29] https://docs.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview

Die meisten Geräte stellten sich als ein Router oder ein Switch heraus und in mindestens einem Fall war der Host ein IBM-Mainframe und ein anderer eine industrielle Kamera. Generell ist zu sagen, dass Telnet im Gegensatz zu sichereren Protokollen wie SSH als nicht geschützt anzusehen ist. Wenn Telnet jedoch unvermeidlich ist, sollten Firewall Access-Control-Listen (ACLs) und andere Kontrollen verwendet werden, um zu beschränken, welche Internet-IP-Adressen auf die Geräte zugreifen können. Da unser Befragungsprozess Verbindungen von mehreren IPs aus aufbauen musste – in einigen Fällen in verschiedenen Ländern – um einen Dienst validieren zu können, sind wir zu dem Schluss gekommen, dass die ACLs wahrscheinlich nicht vorhanden waren oder übermäßig breit ausgelegt waren.

Wenn wir uns die untersuchten Protokolle und Branchen ansehen, können wir feststellen, dass es bestimmte Hotspots gibt.

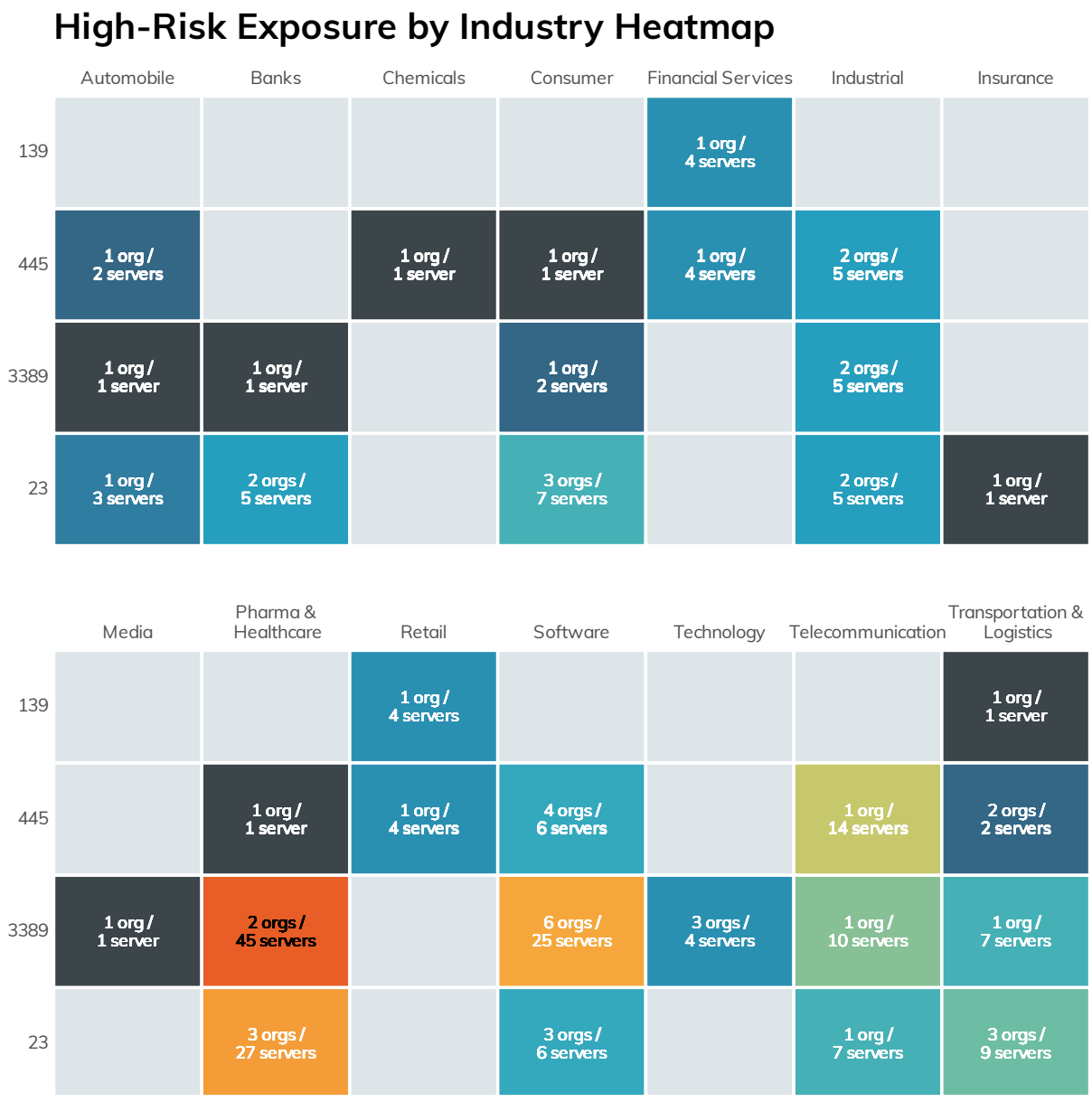


Abb. 16: High-Risk Exposure by Industry Heatmap

Obwohl die meisten der RDP-Exponierungen erstaunlicherweise in der Pharma- und Gesundheitsversorgungsbranche liegen, und nicht etwa in der Informationstechnologie, sollten wir dabei bedenken, dass dies zum Großteil auf die enormen Auswirkungen nur eines Unternehmens zurückzuführen ist, das wir aus offensichtlichen Gründen nicht nennen werden. Ein Pluspunkt, wenn wir den Cloud- und ISP-Netzwerkbereich außer Acht lassen, war, dass bei 280 der DB 314-Unternehmen diese Dienste nicht auf den Standard-Ports zu finden waren.

Fazit für den CISO

Die Ergebnisse deuten darauf hin, dass selbst einige der Unternehmen mit den größten Ressourcen ihre Dienste exponieren, die von Risiken überproportional betroffen sind.

Um die oben genannten Risiken einzudämmen, empfehlen wir nicht die Implementierung von fortgeschrittenen Sicherheitskontrollen oder Software, sondern vielmehr die Rückkehr zu den Grundlagen. Die Risiken entstehen alle in den Anfängen der CIS Top 20[30] Kontrollen.

- Entwickeln und warten Sie einen Bestand aus ins Internet gerichteten Hosts, zu denen Software-Versionen, Rollen und Dienstleistungen gehören, die erwartungsgemäß exponiert werden, sowie den Beweggr- und dafür. Stellen Sie sicher, dass dieser Bestand von externen Scans aller Ihrer öffentlich zugänglichen IP-Bereiche validiert werden kann.
- Implementieren Sie Sicherheitsrichtlinien und Konfigurationsstandards, die diese unterstützen, damit die Verwendung von sicheren Protokollen und Konfigurationseinstellungen eingehalten wird. Am Beispiel von Telnet sollte demnach jedes Gerät, das derzeit Telnet nutzt, SSH unterstützen – und wenn es das nicht kann, ist es zu alt oder unsicher, um direkt mit dem Internet verbunden zu sein.
- Stellen Sie sicher, dass Software und Hardware auf dem neuesten Stand sind. In vielen Fällen, wie z. B. bei Microsoft Windows, enthält die neuere Software bessere Sicherheitsfunktionen und Kontrollen. Das Fehlen dieser Funktionen in älterer Software kann dazu führen, dass Sicherheitskompromisse eingegangen und kompensierende Kontrollen implementiert werden, was die Komplexität erhöht.

[30] https://www.cisecurity.org/controls/cis-controls-list/

Aufdeckung von Schwachstellen (VDP) bei den Unternehmen der Deutschen Börse 314

Ein besonderer Dank geht an Andreas Galauner, der dafür sorgte, dass unsere regionalen Suchen nach VDPs in Deutschland auf Deutsch erfolgten.

Jedes Großunternehmen der Welt ist ein Technologie-Unternehmen.[31] Es ist undenkbar, dass ein Unternehmen, das Milliarden Euro an Umsatz generiert und Tausende von Mitarbeitern weltweit beschäftigt, seine Produkte, Prozesse und Logistik nicht durch beträchtliche Technologieinvestitionen unterstützt. In jedem Aspekt des modernen Lebens vertrauen wir auf fortgeschrittene Technologie. Natürlich wird jeder, der diese Technologien irgendwann mal analysiert hat, wissen, dass wir routinemäßig von Schwachstellen geplagt sind, insbesondere wenn es um internetbasierte Technologie geht.

Wir verfügen jedoch über eine leistungsstarke und bewährte Methode, um der Flut von Schwachstellen in bedeutender Technologie etwas entgegenzusetzen: Coordinated Vulnerability Disclosure[32] (CVD) und der mittlerweile zur Teilnahme an CVD anerkannte Standardmechanismus der VDP[33] (kurz für Vulnerability Disclosure Programs).

Öffentlich zugängliche VDP fehlen ganz augenscheinlich in den meisten Unternehmen der DB 314, was es wiederum den Unternehmen erschwert, auf konstruktive Weise Schwachstellen in ihren Produkten und der technischen Infrastruktur zu erkennen.

Obwohl VDPs in US-amerikanischen Unternehmen der Fortune 500 heute häufiger (etwa 20 %) vorhanden sind, fehlen diese Programme in der DB 314 weitgehend: Nur 34 der börsennotierten Unternehmen (oder etwa 11 %) haben ein erkennbares VDP. Ohne die Programme zur Aufdeckung von Schwachstellen vermitteln sie unbewusst oder auch bei vollem Bewusstsein den Eindruck, dass sie ihre eigenen Schwachstellen nicht erkennen wollen, trotz der Gefahren für Aktionäre wie Kunden.

In dieser Studie suchten wir nach VDPs im Umfeld der DB 314 gelisteten Unternehmen und der Flaggschiff-Marken dieser Unternehmen, und zwar auf ähnliche Weise, als würden wir Schwachstellen über die Produkte und Dienstleistungen dieser Unternehmen offenlegen wollen. Speziell haben wir in der angegebenen Reihenfolge nach Folgendem gesucht:

- Anwesenheit eines VDP in Verbindung mit allen ASX 200 börsennotierten Unternehmen (oder Flaggschiff-Marken dieser Unternehmen), die entweder auf den Bugcrowd[34] oder HackerOne[35] Bug-Bounty-Crowdsourcing-Listen oder in der Disclose.io[36] Programmdatenbank stehen.
- Vorhandensein einer standardisierten security.txt Datei zu jeder Unternehmens- oder Markenwebsite, um die Freigabe von entdeckten Schwachstellen mit Website-Betreibern zu erleichtern.
- Offensichtlicher Indikator eines VDP bei den betreffenden Unternehmen, indem die Begriffe „Vulnerability“ (Schwachstelle), „Disclosure“ (Offenlegung) und „Security“ (Sicherheit) sowie der Firmenname und die Flaggschiff-Marke in Google eingegeben wurden.

[31] https://www.wsj.com/articles/every-company-is-now-a-tech-company-1543901207
[32] https://blog.rapid7.com/2018/10/31/prioritizing-the-fundamentals-of-coordinated-vulnerability-disclosure/
[33] https://blog.rapid7.com/2016/11/28/never-fear-vulnerability-disclosure-is-here/
[34] https://www.bugcrowd.com/bug-bounty-list/
[35] https://hackerone.com/directory/programs
[36] https://github.com/disclose/diodb/

Die erste Untersuchung wurde Ende April 2021 durchgeführt. Diese Recherchen erfolgten in Deutschland in sowohl der englischen als auch der deutschen Version von Google durch einen deutschen Muttersprachler, den Rapid7-Forscher Andreas Galauner. Interessanterweise war der englischsprachige Suchvorgang etwas häufiger in der Lage, VDPs zu finden, als die deutschsprachige Suche. Am Ende können wir vermuten, dass einige der untersuchten Unternehmen, die augenscheinlich kein VDP verwenden, in der Tat einen Prozess einsetzen, um Intelligence über Schwachstellen zu erhalten, aber die Unmöglichkeit, auf einfache Weise ein VDP (in entweder der bevorzugten Firmensprache oder auf Englisch) zu finden, mindert die Wirksamkeit des VDP für sowohl den Recherchierenden als auch die Unternehmen drastisch.

Die Bewertung der relativen Vorzüge der einzelnen VDPs sprengt den Rahmen dieses Berichts, aber wir möchten darauf hinweisen, dass nicht alle VDPs gleich sind – einige bieten bei der Meldung und Bekanntgabe von Schwachstellen robusten „Safe Harbor" Schutz für Forscher und für jene, die zufällig darauf stoßen. Andere möchten Forscher zu stark einschränkenden Vereinbarungen verpflichten, mit denen geregelt wird, was bewertet werden kann und wie die Ergebnisse zu handhaben und zu kommunizieren sind. Für den Zweck dieses Berichts gilt die bloße Existenz eines VDP, unabhängig davon, wie freizügig oder restriktiv es ist, als ein Pluspunkt.

Ergebnisse: Verbreitung der VDP-Akzeptanz

Im Januar 2019 schrieb der australische Bugcrowd-Gründer Casey Ellis in einem Blog-Post, dass „nur 9 % der Fortune 500-Unternehmen Programme zur Aufdeckung von Schwachstellen ausführen".[37] Genau das trifft, laut unseren Untersuchungen, auf Deutschland im ersten Halbjahr 2021 zu. Wir konnten insgesamt 34 Schwachstellen-Aufdeckungsprogramme in den 314-notierten Unternehmen entdecken, die wir im April 2021 untersucht haben, was etwa 11 % der DB 314-Unternehmen ausmacht.

Bei einer so geringen Rate ist es schwierig, zu sagen, ob eine einzelne Branche oder ein untersuchtes Quintil ihre/seine Praxis der Bekanntmachung eines VDP normalisiert hat – die in dieser Schnittmenge vertretenen Branchen sind die Autobranche (6), Banken (1), Chemie (2), Industrie (5), Medien (1), Pharma und Gesundheitsversorgung (3), Einzelhandel (4), Software (5), Technologie (3) und Telekommunikation (3), was ein ziemlich repräsentativer Querschnitt der ganzen DB 314 ist.

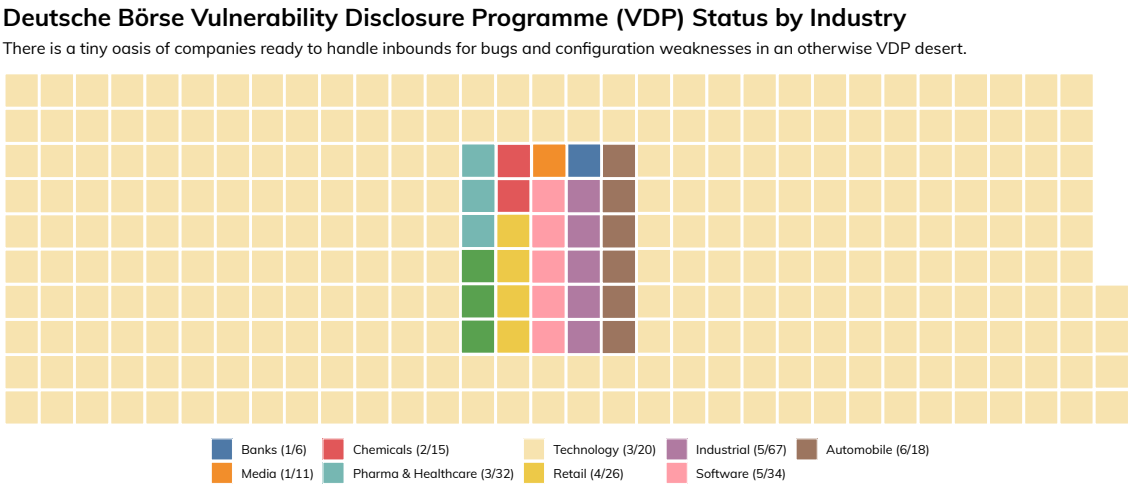


Abb. 17: Deutsche Börse Vulnerability Disclosure Programme (VDP) Status by Inudstry

[37] https://www.bugcrowd.com/blog/3-reasons-why-every-company-should-have-a-vdp/

Das Fazit aus dieser Erkenntnis über die DB 314 ist, dass fast 90 % der deutschen Spitzenunternehmen kein offizielles Programm zur Aufdeckung von Schwachstellen haben, obwohl alle großen Unternehmen einige technische Komponenten verwenden (und daher technische Schwachstellen aufweisen). In vergangenen Jahrzehnten mag diese Gegebenheit nachvollziehbar gewesen sein, aber in der heutigen hypertechnischen Geschäftswelt ist es einfach nicht mehr akzeptabel.

Der Mangel an VDPs in den oberen Schichten der deutschen Wirtschaft wirkt sich abschreckend auf eine vernünftige und verantwortungsvolle Offenlegung von neu entdeckten Schwachstellen in ihren Produkten, Dienstleistungen und Infrastruktur aus – schließlich sind VDPs nicht nur zur Meldung von Software-Bugs in Softwareanwendungen gedacht, sondern dienen auch der Meldung einer Exponierung sensibler Daten über Kunden oder interne Unternehmensprozesse in einem unsicheren Cloud-Speicher. Natürlich ist es möglich, Unternehmen in Branchen ohne formelles VDP Schwachstellen aufzuzeigen, aber der Mangel an VDPs bewirkt Ineffizienz in den Unternehmen und rechtliche Risiken für die Forscher.

Abschließend zeigt ein funktionsfähiges VDP, dass das jeweilige Unternehmen in sein gesamtes IT-Sicherheitsprogramm investiert hat, und das führt zu dem Schluss, dass der Mangel eines VDP genau das Gegenteil signalisiert. Jedes Unternehmen in dieser Liste verwendet eine Datenschutzrichtlinie auf seiner Website, daher sollte jedes Unternehmen eine formelle Methode zum Erhalt und der Bearbeitung von Schwachstellenberichten haben.

Fazit für den CISO

Hoffentlich waren wir als Autoren dieses Berichts in der Lage, unsere starke Befürwortung von klar definierten, leicht erkennbaren Programmen zur Aufdeckung von Schwachstellen aufzuzeigen. Wir sind der Auffassung, dass jedes Unternehmen der DB 314 (und darüber hinaus) eines implementieren sollte.

Der Start und die Ausführung eines erfolgreichen VDP mag kompliziert sein. Schließlich setzt der Einsatz eines VDP einen Sicherheits-Reifegrad voraus, der möglicherweise in dem jeweiligen Unternehmen noch gar nicht vorhanden ist. CISOs in Organisationen ohne VDP wird daher wärmstens empfohlen, sich mit den Grundlagen der Aufdeckung von Schwachstellen vertraut zu machen.

Unserer Ansicht nach gibt es eine kritische Masse von CISO-Fachwissen, was den Aufbau und die Instandhaltung von VDPs betrifft, und ebenso gibt es viele Gelegenheiten, von den Erfahrungen anderer in diesem Bereich zu lernen. Wir haben die Erfahrung gemacht, dass CISOs in der Regel gerne über ihre VDP-Erkenntnisse sprechen, und wenn sie erst einmal anfangen, hören manche ungern wieder auf.

ISO 29147[39] (Informationstechnik – Sicherheitstechniken – Offenlegung von Schwachstellen) und ISO 30111[40] (Informationstechnik – IT-Sicherheitsverfahren – Prozesse für die Behandlung von Schwachstellen) sind ausgezeichnete Ansatzpunkte zum Aufbau, zur Instandhaltung und Verbesserung eines Programms zur Aufdeckung von Schwachstellen. Diese ISO-Vorgaben wurden in Zusammenarbeit mit international anerkannten Experten im Bereich der Aufdeckung von Schwachstellen entwickelt und sind für jeden CISO ausgesprochen hilfreich.

[38] https://www.iso.org/standard/72311.html
[39] https://www.iso.org/standard/69725.html
[40] CISOs können sich weiter informieren unter https://securitytxt.org/

Ein weiterer erster Schritt zur Einrichtung eines minimalen VDP ist ein Kontakt- und Richtliniendokument in `<hxxps://your-company.com/.well-known/security.txt>`. Dies ist ein relativ neuer Standard für die VDP-Kommunikation, der in Signalfunktion grundlegende Kontaktangaben bereitstellt, die sowohl von Menschen als auch von Maschinen gelesen werden können.

Zusammenfassung

RAPID7

Die globale Coronapandemie zwang viele dieser Unternehmen, in kurzer Zeit auf eine große mobile Belegschaft umzusteigen, die im Homeoffice tätig war. Jedes Unternehmen hat für sich Wunder vollbracht, um angesichts einer so drastischen und beispiellosen Veränderung am Arbeitsplatz zu überleben. Darüber hinaus sind deutsche Unternehmen sehr gut darin, gefährlich exponierte Dienste zu beseitigen.

Allerdings blieben diese Unternehmen in vier anderen Bereichen, die wir für diesen Bericht erfasst haben, weit hinter ihren internationalen Kollegen zurück. Mehr Fortschritt muss sein, und er muss schneller erfolgen. Aufgrund ihrer übergroßen Stellung in der deutschen Geschäftswelt haben sie auch Zugang zu den besten und hellsten Köpfen der Cybersicherheit weltweit, und daher ist es selbstverständlich, dass sie sich als Vorzeigemodelle des Internetbürgers verhalten. Die Wissenschaftler bei Rapid7, die an diesem Bericht mitwirkten, hoffen, dass diese Unternehmen und alle Firmen, die mit ihnen in Geschäftsbeziehung stehen, die hier enthaltenen Informationen und Ratschläge unter dem Aspekt der gemeinsamen Verantwortung für den Sicherheitsfortschritt zugunsten aller Beteiligten als hilfreich erachten.

CISO Handlungen auf einen Blick

In diesem Bericht ging es uns darum, aufzuzeigen, was CISOs bei den DB 314 jetzt tun können, um ihre Exponierung gegenüber den häufigsten, hier besprochenen Problemen zu reduzieren. Zur Erinnerung haben wir diese Empfehlungen hier zusammengefasst.

E-Mail-Sicherheit: Wenn Sie auf dem Pfad der domänenbasierten Message Authentication, Reporting & Conformance (DMARC) sind, wie etwa 39 % der DB 314, ist das großartig. Jetzt ist es an der Zeit, herauszufinden, wie Sie von einem `p=none` auf eine `p=quarantine` Richtlinie und letztlich auf eine `p=reject` Richtlinie umsteigen. Das ist kein einfacher Weg, da Sie sicher auf versteckte Schatten-IT stoßen werden, die ihre eigene E-Mail-Infrastruktur betreibt, aber das Vertrauen, das daraus entsteht, E-Mail aus Ihren bedeutenden Markendomänen authentifizieren zu können, ist nicht zu unterschätzen, und auch eine gute Nachricht, die Sie Ihrem Vorstand mitteilen können.

Web-Sicherheit: HTTP Strict Transport Security (HSTS) wird schnell zur Voraussetzung, um eine relativ sichere Website zu betreiben. Sie ist ein Beispiel einer Sicherheitsfunktion, die Browseranbieter wie Google, Apple, Microsoft und Mozilla in zukünftigen Versionen von Chrome, Safari, Edge und Firefox durchsetzen werden. Sie stellt einen relativ einfachen Wechsel dar, den CISOs umsetzen können (verglichen mit den vielen Wunschoptionen aus der Cybersicherheit). Nehmen Sie sich also etwas Zeit, um zu erfahren, ob Ihr Unternehmen HSTS verwendet, und falls nicht, warum nicht?

Unterschiedliche Versionen: In Großkonzernen, die den Kapitalismus prägen, treten im Laufe eines Jahres ziemlich häufig Fusionen und Akquisitionen auf. Das bedeutet, dass der CISO eines DB 314-Unternehmens das Thema Versionskontrolle im Unternehmen niemals wirklich „abgeschlossen“ hat, selbst wenn in eine ausgezeichnete Toolkette zur Verwaltung der Assets und Schwachstellen investiert wurde. Ihrer Struktur werden neue Netzwerke und Netzwerkdienste beitreten, und das bedeutet, dass diese neuen Assets beständig modernisiert und normalisiert werden müssen. Sich dieser kontinuierlichen Aufgabe zu widmen, zahlt sich in einem einfacheren, übersichtlichen Plan für den nächsten Patch-Zyklus aus, ganz gleich, ob der geplant oder völlig überraschend eintritt.

Riskante Services: Telnet, SMB und RDP sollten der Welt da draußen gegenüber niemals direkt exponiert werden. Sie sind nur eine Einladung für den nächsten selbstreplizierenden Cyberangriff, der das Internet unsicher macht. Eine aktuelle Bestandsaufnahme der exponierten Dienste aus internen und externen Scans ist außerordentlich wichtig und hilft Ihnen, eine straffe Richtlinie für die Netzwerkdienst-Exponierung im Internet durchzusetzen. Wie oben erwähnt, gibt es jedoch bei den DB 314 mit Stand 2021 nur noch sehr wenige dieser exponierten Dienste.

Programme zur Aufdeckung von Schwachstellen: Als CISO haben Sie vielleicht die allerbesten Software-, QA- und Platform-Engineers eingestellt. Aber ohne einen guten Ansatz, um die Entdeckungen von Zehntausenden von talentierten Hackern weltweit zu bündeln, hören Sie vielleicht nie von den kritischsten Schwachstellen in Ihren Produkten und Diensten. Ein VDP ist eine Brücke zu dieser enorm großen Community aus wohlgesonnenen Ermittlern, die ähnliche Ziele verfolgen wie Sie: ein sichereres und besser geschütztes Internet. Indem Sie dieses Programm jetzt in Angriff nehmen, schaffen Sie sich viel Zeit, um Software auf sicherere Weise zu entwickeln. Sie genießen zudem den Vorteil, dass die meiste Pionierarbeit in Form von ISO 29147 und ISO 30111 bereits erledigt ist.

Anhang: Priorisierung in Krisenzeiten

Die Aufdeckung von beiden SolarWinds-betreffenden Schwachstellen aus mehreren Technologiebereichen (und den dazugehörigen Kampagnen), die Herausgabe der Out-of-Band-Patches für Microsoft Exchange in Reaktion auf aktive Ausnutzungskampagnen und die Codecov-Kompromittierung, die zweifellos sehr viele Softwareentwicklungs-CI/CD-Prozesse betreffen wird, haben alle so gut wie jedes IT-Sicherheitsteam in allen Branchen überlastet. Wir wollten die Chance nutzen, um zu gewährleisten, dass Sie auf festerem Boden stehen und zugleich die einzelnen Abschnitte in Zusammenhang zu einigen der Krisen setzen, die wir in diesem Jahr bereits bewältigen mussten.

Der Fall von SolarWinds und Codecov hat Drittanbieter-Risiken so klar wie noch nie zuvor in den Fokus gerückt. Wenn Sie eine solide Liste von Partnern/Anbietern und einen aktuellen Kontaktplan haben (was für viele Unternehmen zutrifft), ist es möglich, dass Sie diesen Teil der erweiterten Vorfälle ziemlich gut überstanden haben. Falls nicht, hoffen wir, dass Sie ausreichend Support hatten, um vorausblickend diese Vorkehrungen für nachfolgende schwerwiegende Schwachstellenaufdeckungen und Exploit-Kampagnen umzusetzen.

Wenn es darum geht, herauszufinden, welchen Wert ein Partner/Anbieter auf Sicherheit und Resilienz legt, empfehlen wir Ihnen die Tipps aus dem Abschnitt „CISO-Erkenntnisse“. Sie werden nachts besser schlafen, wenn Sie wissen, dass der Großteil Ihrer Dritt-Kontakte die E-Mail-Sicherheit priorisiert, es vermeidet, gefährliche Dienste im Internet offenzulegen und sowohl beim Patching als auch bei den fortgeschrittenen Verschlüsselungsstandards auf dem neuesten Stand ist. Sie werden auch wissen, wie Sie mit ihm in Verbindung treten können, wenn Sie ein Sicherheitsproblem mit einem seiner Produkte und Dienste entdecken, da der Dritte ein Programm zur Aufdeckung von Schwachstellen verwendet.

Auf vergleichbare Weise zeigten die enorme Exchange-Schwachstelle und damit verbundene bösartige Kampagnen, wie schnell nur eine Schwachstelle in einer Komponente, die Hunderttausende von Unternehmen einsetzen, völlig aus dem Nichts auftreten und selbst den ausgeklügelsten IT-Sicherheitsplan in Unternehmen außer Kraft setzen kann. Eine aktuelle, genaue Telemetrie von allem, was intern und extern eingesetzt wird, kann neben sehr agilen Qualitätssicherungs- und Change-Management-Prozessen (wie im Abschnitt zur Versionsvielfalt vermerkt) den entscheidenden Unterschied machen, ob Sie einen unerwarteten Patch (wie Exchange) schnell mit einer kurzen Bestandsaufnahme abwickeln (nur um zu sehen, ob der Angreifer Zeit hatte, Sie anzugreifen), oder ob Sie einen massiven „alle Mann an Deck“ Vorfall erleben.

Wir hoffen, dass Sie unsere Quantifizierung, den geschaffenen Kontext und unsere Ratschläge nutzen können, während Sie sich nach zwei großen Vorfällen gegen die restlichen Herausforderungen wappnen, denen wir 2021 und darüber hinaus noch begegnen werden.