Umgang mit den kritischen Sicherheitslücken der Microsoft Exchange Server

Wie Sie Ihr System sichern oder auf einen Vorfall reagieren

perseus.
Cybersicherheit auf den Punkt

Inhaltsverzeichnis

01 . Grundinformationen zu den kritischen Sicherheitslücken — Seite 04

Was ist das Problem? — Seite 04

Wie wurden diese Sicherheitslücken bisher ausgenutzt? — Seite 04

Warum sind diese Sicherheitslücken kritisch? — Seite 04

Welche Systeme sind betroffen? — Seite 05

02 . Was tun, um Ihr System akut zu sichern? — Seite 06

Angriffsrelevante Außenverbindungen sperren — Seite 06

Microsoft Patches installieren — Seite 06
• Die Patches können nicht installiert werden? Eine Alternative

Alle Passwörter ändern — Seite 07

Zusätzliche Sicherheitsmaßnahmen — Seite 07

Überprüfung Ihres Systems auf Kompromittierung — Seite 07
• Durch Microsoft-Skripte
• Durch Viren-Scanner
• Manuelle Überprüfung

03 . Was tun bei Angriffsverdacht? — Seite 09

Als erstes: Nachweise sichern — Seite 09

Weitere Schritte abklären — Seite 09

Jetzt schon berücksichtigen: Eventuelle Meldung nach Art. 33 DSGVO — Seite 09

Tiefgehende Überprüfung und Absicherung des Systems — Seite 10

Inhaltsverzeichnis

04 . Was tun nach einem Vorfall? Seite 10

Neuinstallation der Exchange Server Seite 10

Monitoring und Sicherheitsvorkehrungen Seite 10

Cyber-Awareness und -Sicherheit erhöhen Seite 11

Pflichten nach DSGVO überprüfen Seite 12

Anzeige erstatten Seite 12

05 . Rückblick: Erfahrungen der Perseus' Notfallhilfe im März 2021 Seite 13

06 . 3 Tipps, um Ihr Unternehmen noch besser abzusichern Seite 16

Impressum Seite 17

Anhang Seite 19

01 | Grundinformationen zu den kritischen Sicherheitslücken

Was ist das Problem?

- Ab Anfang Januar 2021 wurde Microsoft von externen Security Unternehmen auf Sicherheitslücken in der E-Mail-Transport-Server-Software „Microsoft Exchange Server" aufmerksam gemacht. Ebenfalls ab Anfang Januar entdeckte eines dieser Security Unternehmen (Volexity) Angriffe, bei denen diese Sicherheitslücken ausgenutzt wurden.
- Später stellte sich heraus, dass die Sicherheitslücken bereits in über 10 Jahre alten Programmcodes der Microsoft Exchange Server zu finden waren.
- Anfang März 2021 veröffentlichte Microsoft die ersten Security-Patches, um die Sicherheitslücken der Microsoft Exchange Server zu schließen.
- Es handelte sich damit um Zero-Day-Sicherheitslücken. Also um Sicherheitslücken, welche bereits vor Bekanntwerden dieser durch den Hersteller der Software aktiv von Angreifern ausgenutzt werden. Das Schließen der Sicherheitslücken erfordert i. d. R. entsprechende Security-Patches, welche erst nach Bekanntwerden vom Hersteller entwickelt werden können. Bis die entsprechenden Security-Patches entwickelt und installiert sind, sind Systeme über diese Sicherheitslücken angreifbar.
- Inzwischen gibt es weitere Security-Patches, um die Sicherheitslücken der Microsoft Exchange Server zu schließen. Unternehmen, welche diese Security-Patches noch nicht installiert haben, sind weiterhin angreifbar.
- Lesenswerte Quellen, falls Sie es genauer wissen möchten:
  - Eine genauere Übersicht des zeitlichen Ablaufs (Stand: 3.2.2021)
  - Blogeintrag des Security Unternehmens Volexitiy zu den Microsoft Exchange Server Sicherheitslücken (Stand 8.3.2021)

Wie wurden diese Sicherheitslücken bisher ausgenutzt?

- Angriffe wurden über die automatisierte Platzierung von „Web Shells" ausgeführt.
- Über diese Hintertüren haben Hacker Zugang zum Server und damit auch indirekt zum Netzwerk, in welchem sich das System befindet.
- Da die Angriffe automatisiert erfolgen, können pro Stunde tausende von Servern attackiert werden.

Warum sind diese Sicherheitslücken kritisch?

- Über diese Sicherheitslücken können Cyberkriminelle sich Zugang zu Ihrem System und all seinen Daten und Komponenten verschaffen. Potentiell kann ein Angreifer sich dann von diesem System über weiterführende Angriffe im angebundenen internen Netzwerk fortbewegen und weitere Systeme kompromittieren.
- Die Sicherheitslücken können aus der Ferne ausgenutzt werden, d. h. es ist weder ein lokaler Zugang zum System noch ein VPN Zugriff notwendig.
- Für einen erfolgreichen Angriff ist keinerlei Authentifizierung erforderlich – weder als normaler Nutzer noch als Administrator.

- Die Sicherheitslücken wurden bereits flächendeckend von Cyberkriminellen ausgenutzt.
- Inzwischen kursieren genaue Beschreibungen von Angriffswegen und mehrere voll funktionsfähige Programme zur Ausnutzung der Sicherheitslücken selbst sowie für die weiterführende Kompromittierung der Systeme, z. B. für die Installation von Ransomware. Dadurch sind weitere Angriffe zu erwarten.

Fazit:

Eine Kompromittierung Ihres Systems ist möglich. Handeln Sie umgehend – auch wenn Sie die Security-Patches direkt nach Erscheinen installiert haben. Denn Ihr System kann bereits vor dem Erscheinen der Security-Patches kompromittiert worden sein.

Welche Systeme sind betroffen?

Prinzipiell gilt: Unternehmen, die ihre Microsoft Exchange Server nicht extra abgesichert haben, sollten davon ausgehen, betroffen zu sein.

Eine vollständige Liste aller betroffenen Systeme finden Sie im Anhang.

Folgende Schwachstellen führen in Kombination zur Verwundbarkeit:

- CVE-2021-26412:
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26412
- CVE-2021-26854:
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26854
- CVE-2021-26855:
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
- CVE-2021-26857:
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857
- CVE-2021-26858:
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858
- CVE-2021-27065:
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065
- CVE-2021-27078:
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27078

Hinweis von Microsoft:
Der cloudbasierte E-Mail-Dienst **Microsoft Exchange Online** ist von den Sicherheitslücken nicht betroffen.

02 | Was tun, um Ihr System akut zu sichern?

Angriffsrelevante Außenverbindungen sperren

- **Sperren Sie sofort den Zugriff auf Ihren Microsoft Exchange Server via Port 443, ein- und ausgehend.** Aktuell erfolgen die meisten Angriffe über HTTPS-Zugriffe auf den TCP-Port 443 zu Microsoft Exchange Servern. Durch seine Sperrung verhindern Sie Angriffe über Web Shells, OWA und Active Sync.
- **Weiteres Vorgehen bzgl. Port 443:**
  - Zugang nur über eine VPN-Verbindung ermöglichen, um den Server vor unbefugten externen Zugriffen zu schützen.
- **Sperren Sie alle Zugangsmöglichkeiten mit Windows Active Directory Credentials als Single Factor.** Sie müssen davon ausgehen, dass Cyberkriminellen Ihre Zugangsdaten bekannt sind. Daher sollten Sie – nach Möglichkeit! – alle Zugänge zu Ihrem Netzwerk vorübergehend deaktivieren, die über Windows Active Directory Zugangsdaten ohne zweiten Faktor (z. B. durch SMS, Authenticator App, Computerzertifikat, Hardware Dongle) authentifiziert werden.
- Dazu zählen z. B.
  - VPN
  - OWA
  - und andere öffentlich erreichbare Services

Microsoft Security-Patches installieren

Falls noch nicht geschehen, installieren Sie sofort die Security-Patches auf dem Microsoft Exchange Server. Gehen Sie dabei in folgender Reihenfolge vor:
1. Exchange Port 443 auf Firewall ein- und ausgehend sperren (falls noch nicht geschehen)
2. Neustarten des Microsoft Exchange Servers
3. Installation der Security-Patches
4. Erneutes Neustarten des Microsoft Exchange Servers

Weitere Details bietet der Update Guide von Microsoft.

Die Security-Patches können nicht installiert werden? Eine Alternative

Die folgende Empfehlung zur temporären Behebung der kritischen Schwachstelle wurde der Aussendung des deutschen BSI mit Klassifizierung TLP:WHITE entnommen.
Unternehmen und Organisationen, welche außer Stande sind, die jeweilige Microsoft-Exchange-Umgebung unmittelbar zu aktualisieren, sollten die folgenden Maßnahmen umsetzen:
1. Deaktivieren Sie die Dienste
   - Unified Messaging (UM)
   - Exchange Control Panel (ECP) VDir
   - Offline Address Book (OAB) VDir Services.

Detaillierte Informationen zum Erstellen der Regeln zur Deaktivierung der Dienste.
2. Deaktivieren Sie nun
   - OWA
   - ActiveSync
   - Mögliche weitere Dienste, welche uneingeschränkt von außen (d. h. über das Internet) erreichbar gemacht wurden.

Dies sollte eine Ausnutzung der Schwachstellen verhindern, bis die Security-Patches von von Microsoft installiert werden können.

Überprüfen Sie die Microsoft Exchange Server mit Hilfe des Exchange On-premises Mitigation Tool (EOMT), bevor die Dienste wieder mit dem Internet verbunden werden. Mehr Informationen finden Sie hier.

Alle Passwörter ändern

Es ist anzunehmen, dass Cyberkriminelle sich durch das Auslesen des LSASS-Prozesses Zugriff auf eine große Anzahl von Benutzeranmeldeinformationen verschafft haben. Daher müssen unternehmensweit alle Passwörter zurückgesetzt werden – von allen Benutzer-, Administrator- und Servicekonten im Active Directory.

Zusätzliche Sicherheitsmaßnahmen

Wir empfehlen: Gehen Sie zunächst davon aus, dass Cyberkriminelle Zugriff auf Ihr System hatten. Ergreifen Sie unternehmensweit die folgenden Sicherheitsmaßnahmen.

- **Warnen Sie proaktiv vor Phishing-Mails**
  Es ist anzunehmen, dass die Angreifer die Adressbücher und viele E-Mail-Konversationen Ihres Unternehmens ausgespäht haben und sie in den folgenden Wochen oder Monaten für Phishing-Kampagnen missbrauchen werden. Davor sollten Sie alle Mitarbeiterinnen und Mitarbeiter Ihres Unternehmens warnen. Ebenso Partnerunternehmen, Zulieferbetriebe sowie Kundinnen und Kunden, deren Informationen missbraucht werden könnten.
- **Erhöhte Wachsamkeit für Security Alerts**
  Wir empfehlen, auftretenden Alarmen in den nächsten vier Wochen mit erhöhter Aufmerksamkeit nachzugehen.
- **Erhöhung der Sichtbarkeit auf den Systemen**
  Um die Sichtbarkeit der Aktivitäten auf den einzelnen Systemen zu erhöhen, sollte Sysmon von der Microsoft Sysinternals Tools-Suite eingesetzt werden. Dies ermöglicht einen detaillierteren Einblick in die Aktivitäten eines Systems und erleichtert die Nachverfolgung von Sicherheitsvorfällen.

Überprüfung Ihres Systems auf Kompromittierung

Alle über das Internet erreichbaren Microsoft Exchange Server sollten auf eine mögliche Kompromittierung untersucht werden.
Die Ausnutzung der Microsoft Exchange Server Sicherheitslücken im Rahmen gezielter Angriffe konnte bereits für Anfang Januar 2021 festgestellt werden – lange bevor die Security-Patches zum Schließen der Sicherheitslücken erschienen. Überprüfen Sie daher auf jeden Fall Ihr System auf Kompromittierungen. Unter anderem um zu verhindern, dass bereits eingeschleuste Schadsoftware zu einem späteren Zeitpunkt aktiv wird.

Falls Sie Anzeichen einer Kompromittierung finden: Dokumentieren Sie Ihr Vorgehen sowie die Ergebnisse und lesen Sie weiter bei „Was tun bei Angriffsverdacht?“

Durch das Exchange On-premises Mitigation Tool (EOMT)

- Das Microsoft-Detektionsskript EOMT untersucht Server nach Indizien eines erfolgreichen Angriffs und versucht gefundene Web Shells direkt zu löschen. Mehr Informationen finden Sie hier.

Durch Viren-Scanner

- Prüfen Sie Ihr gesamtes System (Dateisystem, Registry, Arbeitsspeicher, Prozesse, usw.) mit einem Viren-Scanner auf dem aktuellsten Stand, dem integrierten Microsoft Defender oder dem Microsoft Safety Scanner.
- Achtung: Möglicherweise hat Ihr Virenscanner durch die Sicherheitslücken eingeschleuste Web Shells bereits gefunden und gelöscht. Prüfen Sie daher auch die Viren-Scanner-Logs der letzten Monate.

Manuelle Überprüfung

- Prüfen Sie Ihr System auf alle bekannten Anzeichen einer Kompromittierung durch die Sicherheitslücken des Microsoft Exchange Servers. Die Liste der entsprechenden Indicators of Compromise (IOC) ist hier verfügbar.
- Analysieren Sie die Log-Files und das Dateisystem auf
  - verdächtige Dateien in den Verzeichnissen
  - Auffälligkeiten und Anomalien in den Logs seit dem 03.01.21 (dem Tag, an dem die ersten Angriffe dieser Art gesichtet wurden) bis zum Zeitpunkt der Analyse selbst.
- Überprüfen Sie Verzeichnisse, in denen Web Shells gespeichert sein könnten. Bisher gefundene Web-Shell-Dateinamen:
  - Web.aspx
  - Help.aspx
  - Document.aspx
  - errorEE.aspx
  - errorEEE.aspx
  - errorEW.aspx
  - errorFF.aspx
  - healthcheck.aspx
  - aspnet_www.aspx
  - aspnet_client.aspx
  - xx.aspx
  - shell.aspx
  - aspnet_iisstart.aspx
  - one.aspx
- Untersuchen Sie Pfade nach Web Shells. Bisher wurden Web Shells unter folgenden Pfaden gefunden:
  - C:\inetpub\wwwroot\aspnet_client\
  - C:\inetpub\wwwroot\aspnet_client\system_web\
  - %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\
  - C:\Exchange\FrontEnd\HttpProxy\owa\auth
- Analysieren Sie den ein-und ausgehenden Datenverkehr Ihrer Microsoft Exchange Server, z. B. durch das Log der Firewall.
- Untersuchen Sie das verbundene Active Directory auf veränderte, privilegierte Berechtigungen oder Accounts.

Immer auf dem aktuellen Stand
Das Bundesamt für Sicherheit (BSI) aktualisiert fortlaufend sein Dokument „Microsoft Exchange Schwachstellen – Detektion und Reaktion“ zur Überprüfung der Exchange Server auf Kompromittierung: Informieren Sie sich hier

03 | Was tun bei Angriffsverdacht?

Als erstes: Nachweise sichern

Ihre Überprüfungen oder andere Indizien weisen auf eine Kompromittierung der Microsoft Exchange Server hin? Dann vermeiden Sie zunächst jede Datenveränderung und sichern Sie alle Nachweise z. B. durch eine Vollsicherung des Exchange-Systems. Dadurch ermöglichen Sie rückwirkend eine tiefere forensische Untersuchung. Bewahren Sie diese Sicherungskopie gut und von Ihrem System getrennt auf.

Weitere Schritte abklären

- Beginnen Sie nun mit der Incident Response und orientieren Sie sich an Ihren Ablaufplänen für IT-Sicherheitsvorfälle und Datenschutzverletzungen.
- Ziehen Sie ggf. externe Experten hinzu: Fachleute aus dem Bereich Cybersicherheit oder IT-Forensik z. B. von Perseus. Denn das weitere Vorgehen hängt u. a. davon ab, wie Ihr System kompromittiert wurde, welche Schäden bereits vorliegen und ob weitere Schadprogramme wie Malware, Web Shells und Backdoors installiert wurden.
- Wenden Sie sich an die Zentrale Ansprechstelle Cybercrime (ZAC) der Polizei, um das weitere Vorgehen abzusprechen. Die Kontaktdaten der Ansprechstellen Ihres Bundeslandes finden Sie hier.

Jetzt schon berücksichtigen: Eventuelle Meldung nach Art. 33 DSGVO

Datenpannen müssen Sie bei der zuständigen Datenschutzaufsichtsbehörde melden, sobald ein Risiko für betroffene Personen hinreichend wahrscheinlich ist. Davon ist bei einer festgestellten Kompromittierung der Microsoft Exchange Server aufgrund der bekannten Gefährdungslage auszugehen. **Für die Meldung bei der Datenschutzaufsichtsbehörde haben Sie nur 72 Stunden Zeit.**
Es hat sich bewährt, eine eventuelle Meldung bereits vorzubereiten, während noch abgeklärt wird, ob eine Kompromittierung vorliegt. Erste Hinweise hierzu finden Sie hier.

Tiefgehende Überprüfung und Absicherung des Systems

- In Zusammenarbeit mit internen oder externen Fachleuten aus dem Bereich Cybersicherheit oder IT-Forensik z. B. von Perseus.
- Das Vorgehen ist abhängig vom konkreten Schadensbild
- Ggf. eine vollständige Säuberung des Systems von Schadprogrammen und -codes wie Web Shells (ASPX), Backdoors (Web Shell, Powercat) und Scheduled Tasks.
- Ggf. das virtuelle Verzeichnis für das Offline-Adressbuch (OAB) neu erstellen
- Genaue Überprüfung des verbundenen Active Directory auf Anomalien, z. B. auf neue Accounts oder Account-Änderungen an administrativen Rollen.

04 | Was tun nach einem Vorfall?

Neuinstallation der Microsoft Exchange Server

Da in Einzelfällen über die Sicherheitslücken Trojaner eingeschleust wurden, wird eine Neuinstallation der Microsoft Exchange Server empfohlen.

1. Deaktivieren Sie den Netzwerkzugriff Ihres Microsoft Exchange Servers, z. B. durch Entfernen des Netzwerkkabels (physisches System), oder durch Deaktivieren oder Entfernen des Netzwerkinterfaces (VM).
2. Falls noch nicht geschehen: Sichern Sie den aktuellen (kompromittierten) Zustand Ihres Microsoft Exchange Servers durch Anlegen eines Backups, einer Kopie der virtuellen Maschine, oder durch Anfertigen eines Abbildes.
    1. Im Falle eines physischen Servers können Sie eine Sicherungskopie z. B. über den FTK Imager erstellen. Hier in der Portable Version kostenlos erhältlich.
3. Sichern Sie die Datenbanken des Microsoft Exchange Servers für eine bevorstehende Migration.
4. Installieren Sie den Microsoft Exchange Server neu und halten Sie das System offline bzw. vom Netz getrennt. Aktualisieren Sie das System offline, indem Sie die entsprechenden Security-Patches von Microsoft laden und z. B. über einen Wechseldatenträger auf das System übertragen. Beachten Sie die Reihenfolge bei der Installation von Cumulative Updates (CUs) und den März-Security-Patches.
5. Überprüfen Sie den Schutz Ihres Servers mithilfe des Exchange On-premises Mitigation Tool (EOMT) von Microsoft.
6. Migrieren Sie Ihre Datenbestände.

Monitoring und Sicherheitsvorkehrungen

- **Verfolgen Sie das Logging genauer.** Wir empfehlen:
    - Überprüfen Sie das Log-Level auf Firewalls, Webproxies, Domain-Controller und Intrusion Detection Systemen
    - Erhöhen Sie ggf. den Umfang bzw. das Log-Level vor allem für Microsoft Exchange Server und insbesondere Internetzugriffe. So ermöglichen Sie sich Feinanalysen.

- **Erhöhung der Sichtbarkeit auf den Systemen**
  Um die Sichtbarkeit der Aktivitäten auf den einzelnen Systemen zu erhöhen, sollte Sysmon von der Microsoft Sysinternals Tools-Suite eingesetzt werden. Dies ermöglicht einen detaillierten Einblick in die Aktivitäten eines Systems und erleichtert die Nachverfolgung von Sicherheitsvorfällen.

- **Sperren Sie potentiell gefährliche IP-Adressen.** Ziehen Sie Geo-Blocking für IP-Adressen und IP-Blacklisting in Erwägung. Insbesondere das BSI und Microsoft liefern aktuelle Hinweise zu entsprechenden IP-Adressen.

- **Optimieren Sie Ihre Backups.** Überprüfen Sie Ihre Backup-Strategie und optimieren Sie sie gegebenenfalls. Besonders wichtig ist, mindestens ein Backup für Angreifer unzugänglich zu halten – also getrennt von Ihrem System, z. B. auf einer ausgesteckten externen Festplatte.

- **Überprüfen des Patch Managements.** Arbeiten Sie anhand des konkreten Vorfalls auf, wie gut Ihr Patch Management war. Wann wurden die Security-Patches eingespielt? Gibt es etwas zu verbessern? Wenn nicht: Loben Sie die zuständigen Mitarbeiterinnen und Mitarbeiter für ihr vorbildliches Vorgehen.

Cyber-Awareness und -Sicherheit erhöhen

Nach einem Cyber-Vorfall können erhöhte Sicherheitsrisiken bestehen, z. B. für gezielte Phishing-Angriffe. Zugleich bietet ein Cyber-Vorfall aber auch Möglichkeiten, die Cyber-Sicherheit Ihres Unternehmens zu erhöhen: Durch die Analysen des Systems wurden vielleicht bisher unbekannte Sicherheitslücken entdeckt. Gleichzeitig ist das Thema Cyber-Sicherheit im gesamten Unternehmen sehr konkret und relevant geworden. Für entsprechende Trainings, Maßnahmen, Informationen und Angebote besteht jetzt ein erhöhtes Interesse.

- **Erhöhen Sie die Cyber-Awareness.** Ermöglichen Sie allen im Unternehmen, zu mehr Cyber-Sicherheit beizutragen. Durch gezielte Warnungen, Online-Kurse und weitere Angebote, z. B. von Perseus. So sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter u. a. für den umsichtigen Umgang mit E-Mails, die Erkennung gefälschter E-Mails und den richtigen Umgang mit Auffälligkeiten.

- **Warnen Sie proaktiv vor Phishing-Mails**
  Es ist anzunehmen, dass Cyberkriminelle Zugriff auf E-Mail-Adressbücher und viele E-Mail-Konversationen hatten und sie in den folgenden Wochen oder Monaten für Phishing-Kampagnen missbrauchen könnten. Daher sollten Sie umfassend vor Phishing-Mails warnen – Ihre Mitarbeiterinnen und Mitarbeiter sowie alle potenziell betroffenen Geschäftskontakte wie z. B. zuliefernde Betriebe.

- **Erhöhte Wachsamkeit für Security Alerts**
  Wir empfehlen, auftretenden Alarmen in den nächsten vier Wochen mit erhöhter Aufmerksamkeit nachzugehen.

- **Bereiten Sie optimale Reaktionen vor.** Schaffen Sie beste Voraussetzungen, um unternehmensweit schnell auf zukünftige Sicherheitswarnungen zu reagieren, z. B. auf einen besonders raffinierten Phishing-Angriff.

- **Überprüfen Sie die Cyber-Sicherheit Ihres Unternehmens.** Ob mit einem externen Dienstleister wie Perseus oder mit internen Mitteln – verschaffen Sie sich einen Überblick über empfehlenswerte und bereits ergriffene Cyber-Schutzmaßnahmen Ihres Unternehmens. Hilfreiche Informationen bieten z. B.
  - das BSI mit seinem Überblick „Basismaßnahmen der Cyber-Sicherheit"
  - der Perseus Leitfaden „Cybersicherheit für den Mittelstand"

Pflichten nach DSGVO überprüfen

Falls Ihre Microsoft Exchange Server kompromittiert wurden, müssen Sie genau prüfen, ob Sie den Vorfall der zuständigen Datenschutzaufsichtsbehörde melden müssen – und ob Sie eventuell weitere betroffene Personen benachrichtigen müssen. **Für die Meldung bei der Datenschutzaufsichtsbehörde haben Sie nur 72 Stunden Zeit.**

Erste Informationen haben wir Ihnen hier zusammengetragen, sie stellen jedoch keine Rechtsberatung dar. Bei Unsicherheiten bzgl. der Meldepflicht holen Sie Rechtsrat ein oder kontaktieren Sie Ihre zuständige Datenschutzbehörde.

Wichtige Informationen im Überblick:
- Gesetzestext zur Meldung bei der Aufsichtsbehörde: Artikel 33 der DSGVO
- Eine Meldung ist nicht notwendig, wenn die Kompromittierung „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt." Damit kann jegliches Risiko gemeint sein, auch ein minimales.
- Wichtig aufgrund des 72-stündigen Zeitfensters: **Bei der Meldung geht Geschwindigkeit vor Vollständigkeit.** Aktuell noch nicht vorliegende Informationen können Sie nachliefern – laut Artikel 34 Absatz 4 der DSGVO.
- Welche Datenschutzaufsichtsbehörde ist die zuständige? Für deutsche Unternehmen ist die Aufsichtsbehörde des Bundeslandes zuständig, in dem sich der Unternehmenssitz befindet.
- Welche Inhalte die Meldung mindestens haben muss, steht in Artikel 33 der DSGVO
- Weitere Pflichten nach DSGVO:
  - Benachrichtigung von Betroffenen, wenn die Datenpanne voraussichtlich ein hohes Risiko für sie bedeutet. Details: Artikel 34 der DSGVO.
  - Beseitigung der Datenpanne
  - Dokumentation des Vorfalls

Einige beispielhafte Fallkonstellationen, in denen Meldungen erforderlich oder nicht erforderlich sind, finden Sie auf Seite 7 in diesem Dokument des Bayrischen Landesamts für Datenschutz.

Anzeige erstatten

Eine Kompromittierung bzw. ein Angriff Ihrer Microsoft Exchange Server ist eine Straftat. Erstatten Sie daher Anzeige bei der zuständigen Polizei – auch damit diese Straftat in die Statistik zur aktuellen Lage eingehen kann. Wenden Sie sich dazu an Ihre örtliche Polizeidienststelle.
Für Fragen steht Ihnen die Zentralen Ansprechstelle Cybercrime (ZAC) Ihres Bundeslandes zur Verfügung. Die entsprechenden Kontaktdaten finden Sie hier.

05 | Rückblick: Erfahrungen der Perseus‘ Notfallhilfe im März 2021

So konnten wir helfen:
Bei den Sicherheitslücken der Microsoft Exchange Server handelte es sich um Zero-Day-Exploits. Das heißt, sie wurden bereits ausgenutzt, bevor es Security-Patches gab, um diese Lücken zu schließen.

Umso wichtiger war die zeitnahe, stets aktuelle Kommunikation über unseren Blog und Social Media, unsere Sicherheitswarnungen sowie unsere Notfallhilfe. Unser Fokus lag dabei auf der Warnung vor aktuellen Gefahren und konkreten Anleitungen und Hinweisen, um sie zu mindern.

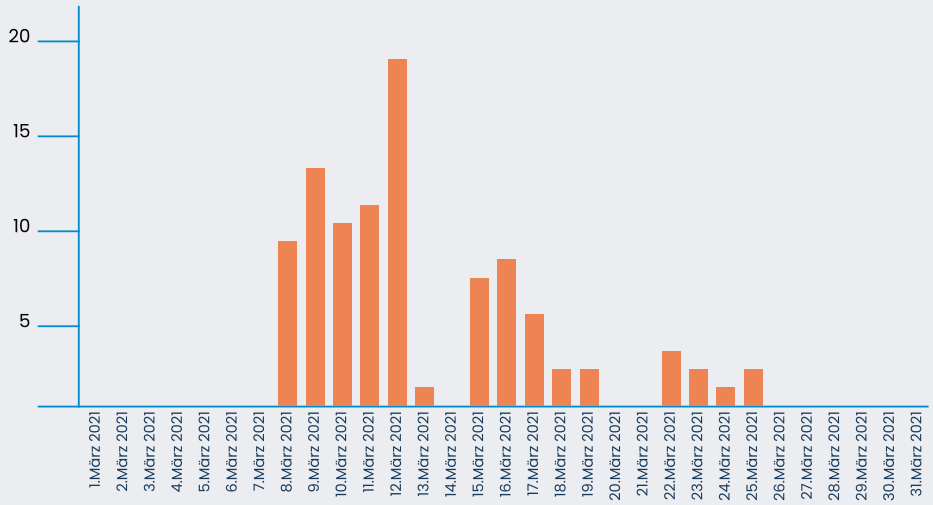
Warnungen, Informationen und Handlungsanweisungen
- 3 Sicherheitswarnungen versendet an alle Perseus-Kunden
- 1 Blogbeitrag (am 09.03.)
- diverse Social Media Updates

Unsere Hilfe bei Not- und Verdachtsfällen im März 2021
- Insgesamt 132 neu gemeldete Not- bzw. Verdachtsfälle

- **Davon wurden 112 aufgrund der Microsoft Exchange Sicherheitslücken gemeldet**

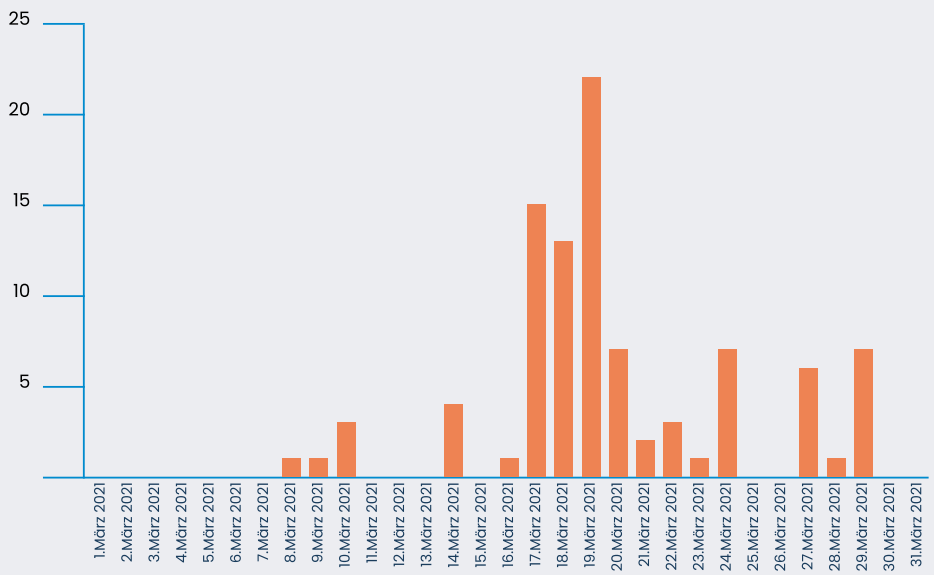
- **Insgesamt 106 abgeschlossene Not- bzw. Verdachtsfälle. 95 von ihnen wurden aufgrund der Microsoft Exchange Sicherheitslücken gemeldet.**

Zeitpunkt der gemeldeten Vorfälle im Zuge der Sicherheitslücken der Microsoft Exchange Server.*

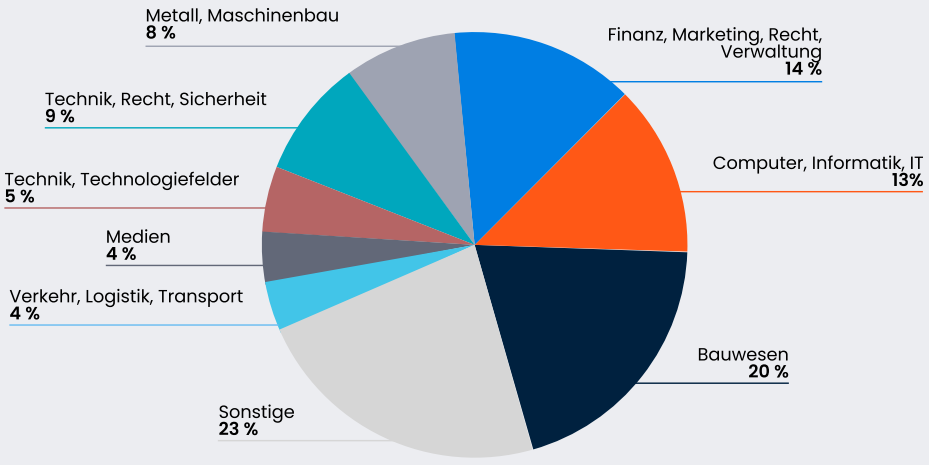


* Betrachtet wurden die bereits gelösten Vorfälle

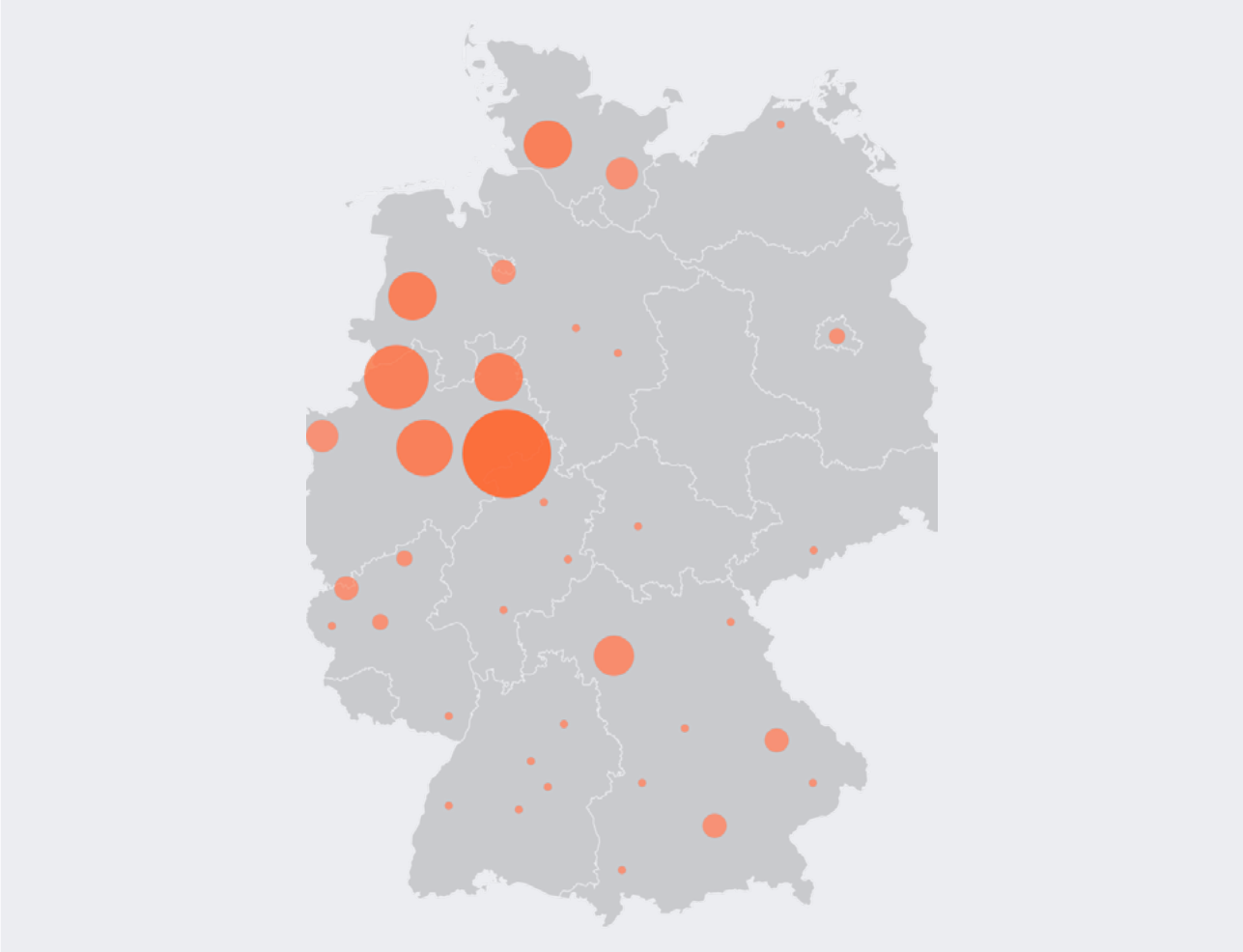
Zeitpunkt der gelösten Vorfälle im Zuge der Sicherheitslücken der Microsoft Exchange Server



Vorfälle nach Branchen der Unternehmen



Geografische Verteilung der uns gemeldeten Vorfälle



Das haben wir gelernt:

- Der Bedarf ist hoch: Viele Unternehmen haben sich mit Bitte um Unterstützung an uns gewandt.
- Oft brauchten die unternehmenseigenen IT-Abteilungen oder externen IT-Dienstleister spezialisierte Unterstützung durch Perseus' Fachleute für Cybersicherheit und IT-Forensik
- Häufige Fragen waren:
  - Was müssen wir jetzt tun?
  - Wie erkennen wir, ob wir betroffen sind?
  - Wer kann für uns analysieren ob ggf. Daten abgeflossen sind oder andere weiterführende Tätigkeiten durch die Angreifer durchgeführt wurden?
  - Worauf müssen wir in der Zukunft achten, damit sowas nicht mehr passiert?
- Die direkte Schadensbehandung nur durch Perseus und den Endkunden ist zeitlich effizienter (durchschnittlich 395 Minuten), als eine Schadensbehandlung, bei der ein externer IT-Dienstleister beteiligt ist (durchschnittliche Bearbeitungszeit 535 Minuten).

Ungewöhnlich schnelle, qualitativ hohe Bearbeitung
Mit 480 Minuten durchschnittlicher Bearbeitungszeit haben wir die Perseus gemeldeten Microsoft Exchange Server Verdachts- bzw. Notfälle enorm schnell bearbeitet. Zum Vergleich: Die durchschnittliche Bearbeitungszeit im Jahr 2020 betrug 18 Stunden pro Vorfall.

Wie war diese Beschleunigung möglich? Wir haben sehr schnell sogenannte Standard Operating Procedures erstellt – also ein standardisiertes Vorgehen. Dadurch konnten wir die Vorfälle außerordentlich effizient und in sehr hoher Qualität abarbeiten.

Fazit:

In Situationen wie dieser brauchen Unternehmen flankierende Unterstützung. Sie müssen aktiv und nachdrücklich gewarnt werden, konkrete Handlungsanweisungen erhalten und wissen, an welche Spezialisten sie sich wenden können. **Genau dafür sind wir von Perseus da.**

06 | 3 Tipps, um Ihr Unternehmen noch besser abzusichern

- **Definieren Sie eine Person, die für Cyber-Sicherheit zuständig ist – und dafür auch Zeit, Budget, Schulungen und Handlungsspielräume erhält.** Dadurch wird sich einerseits die allgemeine Cyber-Sicherheit Ihres Unternehmens erhöhen. In akuten Fällen wie dem Zero-Day-Exploit der Microsoft Exchange Server liegen dann bereits Notfallpläne vor, so dass Sie zeitnah und gezielt reagieren können. Weiterhin können Kompromittierungen schneller erkannt werden, wenn alle im Unternehmen wissen, an wen sie sich bei Unsicherheiten oder in Verdachtsfällen wenden können.

- **Schaffen Sie unternehmensweit Cyber-Awareness – ein Grundbewusstsein für Cyber-Sicherheit.** Ihre Mitarbeiterinnen und Mitarbeiter sind ein unverzichtbarer Schutzfaktor für die Cyber-Sicherheit Ihres Unternehmens. Sie können Angriffsversuche erfolgreich abwehren, technische Kompromittierungen früh erkennen und durch richtige Reaktionen Schäden minimieren. Dazu müssen sie aber wissen, worauf sie achten und was sie tun müssen. Fördern Sie die Cyber-Awareness durch eigene Maßnahmen oder mit Hilfe externer Anbieter wie z. B. Perseus. Weitere Informationen finden Sie hier.

- **Bereiten Sie eine Kontakt-Notfallliste vor.** Sie können schneller reagieren, wenn Ihnen die Kontaktdaten z. B. von Fachleuten für IT-Forensik oder der Perseus Notfallhilfe bereits vorliegen.

- Wir helfen Ihnen bei Ihrem ersten Eintrag, falls Sie noch kein Perseus-Mitglied sind: Diese Notfall-Nummer ist rund um die Uhr erreichbar: **+49 30 233 2730 95**

Impressum

Haftungsausschluss

Haftung für Inhalte
Die Inhalte dieses Whitepapers wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte können wir jedoch keine Gewähr übernehmen. Als Diensteanbieter sind wir gemäß § 7 Abs.1 TMG für eigene Inhalte auf diesen Seiten nach den allgemeinen Gesetzen verantwortlich. Nach §§ 8 bis 10 TMG sind wir als Diensteanbieter jedoch nicht verpflichtet, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werden wir diese Inhalte umgehend entfernen.

Haftung für Links
Dieses Whitepaper enthält Links zu externen Webseiten Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar. Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

Urheberrecht
Die durch die Seitenbetreiber erstellten Inhalte und Werke auf diesen Seiten unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechtes bedürfen der schriftlichen Zustimmung des jeweiligen Autors bzw. Erstellers. Downloads und Kopien dieser Seite sind nur für den privaten, nicht kommerziellen Gebrauch gestattet. Soweit die Inhalte auf dieser Seite nicht vom Betreiber erstellt wurden, werden die Urheberrechte Dritter beachtet. Insbesondere werden Inhalte Dritter als solche gekennzeichnet. Sollten Sie trotzdem auf eine Urheberrechtsverletzung aufmerksam werden, bitten wir um einen entsprechenden Hinweis. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Inhalte umgehend entfernen.

Impressum

Perseus Technologies GmbH | Hardenbergstraße 32 | 10623 Berlin
Telefon: +49 (30) 959998080 | E-Mail: info@perseus.de
Geschäftsführer: Christoph Holle

Handelsregister: Amtsgericht Charlottenburg HRB 180356 B
USt.-Ident-Nr.: DE308271739
Verantwortlicher gem. § 55 Abs. 2 RStV: Christoph Holle

An wen können Sie sich im Notfall wenden?

Unsere Notfallhilfe steht Perseus-Mitgliedern in Verdachtsfällen zur Seite:
https://www.perseus.de/produkt/notfallhilfe/

Für Nicht-Mitglieder ist diese Notfall-Nummer rund um die Uhr erreichbar:
+49 30 233 2730 95

Anhang

Stand 26.03.2021 sind des Weiteren folgende Systeme betroffen:

- Microsoft Exchange Server 2010 (RU 31 for Service Pack 3)
- Microsoft Exchange Server 2013 (CU 23)
- Microsoft Exchange Server 2016 (CU 19, CU 18)
- Microsoft Exchange Server 2019 (CU 8, CU 7)
- Microsoft Exchange Server 2010 Service Pack 3
- Microsoft Exchange Server 2013 Cumulative Update 21
- Microsoft Exchange Server 2013 Cumulative Update 22
- Microsoft Exchange Server 2013 Cumulative Update 23
- Microsoft Exchange Server 2013 Service Pack 1
- Microsoft Exchange Server 2016 Cumulative Update 10
- Microsoft Exchange Server 2016 Cumulative Update 11
- Microsoft Exchange Server 2016 Cumulative Update 12
- Microsoft Exchange Server 2016 Cumulative Update 13
- Microsoft Exchange Server 2016 Cumulative Update 14
- Microsoft Exchange Server 2016 Cumulative Update 15
- Microsoft Exchange Server 2016 Cumulative Update 16
- Microsoft Exchange Server 2016 Cumulative Update 17
- Microsoft Exchange Server 2016 Cumulative Update 18
- Microsoft Exchange Server 2016 Cumulative Update 19
- Microsoft Exchange Server 2016 Cumulative Update 8
- Microsoft Exchange Server 2016 Cumulative Update 9
- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2019 Cumulative Update 1
- Microsoft Exchange Server 2019 Cumulative Update 2
- Microsoft Exchange Server 2019 Cumulative Update 3
- Microsoft Exchange Server 2019 Cumulative Update 4
- Microsoft Exchange Server 2019 Cumulative Update 5
- Microsoft Exchange Server 2019 Cumulative Update 6
- Microsoft Exchange Server 2019 Cumulative Update 7
- Microsoft Exchange Server 2019 Cumulative Update 8