I. QUARTAL, 2021

Allianz

CYBER-NEWSLETTER

Aktuelle Entwicklungen

Mehrere schwerwiegende Schwachstellen in Microsoft Exchange

Microsoft hat am 03. März 2021 außerplanmäßig Sicherheitsupdates sowie eine Sicherheitswarnung für verschiedene Versionen von Microsoft Exchange veröffentlicht. Die durch die Updates geschlossenen Sicherheitslücken werden spätestens seit Januar 2021 gezielt und seit Ende Februar automatisiert u.a. zur Erlangungen von Administrationsrechten ausgenutzt.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat aufgrund der erheblichen Bedrohungslage ebenfalls eine Cybersicherheitswarnung – zeitweise der höchsten Stufe – veröffentlicht.

Wir empfehlen Ihnen dringend zu prüfen, ob Sie verwundbare Versionen von Microsoft Exchange einsetzen und sollte dies der Fall sein unverzüglich dem vom BSI empfohlenen Vorgehen folgen. Aufgrund der dynamischen Lage verweisen wir an dieser Stelle auf die vom BSI eingerichtet Website (auch über den oben angezeigten QR-Code erreichbar).

IN DIESEM QUARTAL

Phishing-Radar: Aktuelle Warnungen zu Phishing

Unter nachfolgendem Link informiert die Verbraucherzentrale Bundesverband über die Aspekte und aktuelle Fälle von Phishing:

Phishing-Radar: Aktuelle Warnungen | Verbraucherzentrale.de

Angriffe über Windows RDP Server

Windows RDP Server werden für DDoS-Angriffe missbraucht

Windows RDP Server, die auf einem bestimmten Port (UDP-Port 3389) laufen, können in DDoS-Botnetze eingeschleust und von Angreifern dazu genutzt werden, Anfragen an Opfernetzwerke weiterzuleiten und zu verstärken.

Die Angreifer senden hierbei modifizierte Datenpakete an UDP-Ports von Windows RDP Servern, die diese dann – als DDoS-Angriff – an Opfernetzwerke senden. Hierbei werden die modifizierten Datenpakete in ihrer Größe verändert, was zu einer „Verstärkung“ des Angriffs führt.

Dieses Vorgehen wird von Sicherheitsforschern als DDoS-Verstärkungsfaktor bezeichnet und ermöglicht es Angreifern mit Zugang zu begrenzten Ressourcen, groß angelegte DDoS-Angriffe zu starten, indem Sie Junk-Traffic mit Hilfe von im Internet exponierten Systemen verstärken. Nach einer anfänglichen Phase des Einsatzes dieser Methode durch erfahrene Angreifer, wurde diese nun auch einem Arsenal an sogenannter DDoS-for-hire-Services hinzugefügt und somit die Reichweite und Nutzbarkeit auch durch unerfahrene Angreifer entsprechend erhöht.

Derzeit hat die Sicherheitsfirma Netscout nach eigenen Angaben weltweit mehr als 33.000 Windows RDP Server erkannt, welche über das Internet erreichbar sind und auf dem „angreifbaren“ UDP-Port 3389 laufen. Daher sollten Systemadministratoren, die Windows RDP Server betreiben, diese entweder offline nehmen oder auf den entsprechenden TCP-Port umstellen und durch VPNs (Virtual Private Network) schützen.

Task Force überprüft die Verwendung von US-Clouddiensten bzgl. Datenschutz

Deutschen Unternehmen drohen verschärfte Kontrollen wegen des Datentransfers personenbezogener Nutzerdaten in die USA. Die Mehrheit der deutschen Datenschutzbehörden beteiligt sich an einer Task Force unter der Leitung von Hamburg und Berlin, welche den “Vollzug” der Anforderungen des Schrems-II-Urteils bundesweit bei Unternehmen stichprobenartig kontrolliert. Dabei wollen die Behörden Unternehmen auswählen, bei denen der Grund zur Annahme besteht, dass sie Dienstleister aus Drittstaaten verwenden.

Im sogenannten Schrems-II-Urteil hatte der Europäische Gerichtshof im Juli 2020 das Datenschutzabkommen Privacy Shield zwischen der EU und den USA für unzulässig erklärt.

Dem Urteil zufolge sind sogenannte Standarddatenschutzklauseln zwar zulässig, doch im Falle der USA dürften diese aktuell nicht ausreichen. Die EU-Kommission hat inzwischen neue Entwürfe vorgelegt, die den Datenschützern aber noch nicht in jeder Hinsicht genügen.

Nach Angaben der Hamburger Datenschutzbehörde stehen die konkreten Auswahlkriterien für die Stichprobenkontrollen noch nicht fest, werden jedoch derzeit final abgestimmt. Soweit bereits konkrete Beschwerden gegen einzelne Stellen vorliegen, sind die Aufsichtsbehörden gegenwärtig schon in Prüfverfahren eingetreten. Datenschützer sehen betroffene Firmen einem erheblichen rechtlichen Risiko ausgesetzt.

Phishing-Radar: Aktuelle Warnungen zu Phishing

Unter nachfolgendem Link informiert die Verbraucherzentrale Bundesverband über die Aspekte und aktuelle Fälle von Phishing:

Phishing-Radar: Aktuelle Warnungen | Verbraucherzentrale.de

Datenschutz Bußgelder

Datenschützer verhängen deutlich mehr Bußgelder

Im vergangenen Jahr sind deutlich mehr Bußgelder wegen Verstößen gegen die EU-Datenschutz-Grundverordnung (DSGVO) verhängt worden. Einer Umfrage des Handelsblatts unter den Datenschutzbeauftragten des Bundes und der Länder zufolge wurden 301 Bußen ausgesprochen. Das entspricht einem Anstieg um 60% im Vergleich zum Jahr 2019. Die Summe der verhängten Bußgelder beläuft sich auf rund 48 Millionen Euro (diese sind teilweise noch nicht rechtskräftig).

Die meisten Geldstrafen wegen Datenschutzverstößen verhängte die Behörde in Nordrhein-Westfalen mit 93 Bußgeldern. Gefolgt von Thüringen mit 41, Sachsen (29), Niedersachsen (27), Hamburg (22), Berlin (21), Baden-Württemberg (19), Brandenburg (16), Sachsen-Anhalt (14), Rheinland-Pfalz (7), Saarland (6), Bayern (4) und Hessen (2).

Das höchste Bußgeld in Höhe von 35,3 Millionen Euro wurde gegen den Modehändler Hennes & Mauritz erlassen. Das zweithöchste Bußgeld des vergangenen Jahres in Höhe von 10,4 Millionen Euro wurde gegen den Online-Elektronikhändler Notebooksbilliger.de erlassen. Auf Platz 3 rangiert ein Bußgeld in Höhe von 1,2 Millionen Euro gegen die AOK in Baden-Württemberg.

Auch die Zahl der Datenpannen hat dem Bericht des Handelsblatts zufolge drastisch zugenommen. Demnach registrierten die Behörden des Bundes und der Länder im vergangenen Jahr 26.260 Pannen.

Passwörter sicher verwalten Teil I

Passwortmanager im Test

Es gibt einige Methoden, um Passwörter nicht zu vergessen, doch je mehr Benutzerkonten anfallen, desto schwieriger wird es. Passwortmanager entlasten das Gedächtnis und steigern die Sicherheit, denn wer sich die Passwörter nicht selber merken muss, kann für jeden Zweck ein starkes und individuell generiertes Passwort benutzen.

Ein guter Passwortmanager bringt idealerweise eine Browsererweiterung mit, die Login-Felder im Webbrowser automatisch oder per Mausklick ausfüllt. Die Passwortdaten werden von der Software (Passwortmanager) erfasst, sobald sich der Nutzer zum ersten mal einloggt, und legt die Anmeldedaten in einer eigenen verschlüsselten Datenbank ab.

Die meisten Programme speichern außer Passwörtern auch noch andere wichtige Daten (z.B. Kontaktdaten, Bankkonto-Daten, persönliche Notizen etc.). Einige Passwortmanager schätzen zusätzlich noch die Qualität des hinterlegten Passworts ein, indem sie die Länge und die Zusammensetzung des Passwortes analysieren und teilweise prüfen, ob das gleiche Passwort bei mehreren Diensten genutzt wird.

Einige Produkte bieten zusätzlich eine als „Darknet-Überwachung“ beworbene Funktion an, in dem sie prüfen, ob Logins schon einmal abhanden gekommen sind und geben eine entsprechende Warnung aus. Hierbei handelt es sich im Grunde um eine Abfrage bei einem Dienst wie HavelBeenPwned.com.

Phishing-Radar: Aktuelle Warnungen zu Phishing

Unter nachfolgendem Link informiert die Verbraucherzentrale Bundesverband über die Aspekte und aktuelle Fälle von Phishing:

Phishing-Radar: Aktuelle Warnungen | Verbraucherzentrale.de

Passwörter sicher verwalten Teil II

Für einen Passwortmanager sind Datenschutz und Sicherheit substantiell – immerhin vertraut man ihm den Zugang zum eigenen digitalen Leben an. Doch in einigen Passwortmanagern – unabhängig davon, ob diese kostenpflichtig sind oder nicht – stecken sogenannte Trackingdienste, welche man bei einem Passwortmanager nicht verwendet sehen will.

Allein aus Sicherheitsgründen will man keine Dateien von Drittanbietern (Trackingdienste) in einem Passwortmanager haben, von denen man nie so genau weiß, was sie eigentlich zu welchem Zeitpunkt für Daten absaugen oder anfragen und welche Sicherheitslücken sie eventuell mitbringen. Eine Untersuchung durch Sicherheitsforscher hat ergeben, dass wenn z.B. ein neues Passwort angelegt wird, der Passworttyp (z.B. Passwort, Bankdaten, Adresse etc.), das Erstellungsdatum, die IP-Adresse und eine weitere Fülle von Daten des verwendeten Geräts durch die Trackingdienste gesammelt und an den Hersteller bzw. den Trackingdienstanbieter übermittelt werden.

Allerdings gibt es hier auch Ausnahmen. Passwortmanager wie z.B. 1Password oder Keepass sind (zum Zeitpunkt der Erstellung dieses Newsletters) Trackingdienst-frei. Diese bringen teilweise keine Cloud- und Synchronisationsdienste mit – was aber auch ein Vorteil sein kann. Denn bei Cloud-Passwortspeichern muss man sich zwar um die Passwortsynchronisation nicht selbst kümmern, jedoch gibt man die Kontrolle darüber in die Hand eines Dritten – in diesem Fall dem Clouddienst-Anbieter.

Fazit

Ob nun kostenpflichtige oder kostenfreie Passwortmanager genutzt werden, welche Daten über einen Cloud-Anbieter synchronisiert oder nicht synchronisiert werden, muss letztendlich jeder Nutzer selbst entscheiden.

Die Hauptsache ist, dass Passwortmanager verwendet werden und jeder Nutzer so eine Möglichkeit hat für jede Anwendung ein individuelles und komplexes Passwort vergeben zu können ohne sich dieses merken zu müssen.

Phishing-Radar: Aktuelle Warnungen zu Phishing

Unter nachfolgendem Link informiert die Verbraucherzentrale Bundesverband über die Aspekte und aktuelle Fälle von Phishing:

Phishing-Radar: Aktuelle Warnungen | Verbraucherzentrale.de