braincon


# Wie sind Ihre Postfächer geschützt?

Es geht um weit mehr als nur die Postfächer

## Microsoft Exchange Zero-Day Sicherheitslücke

Schluss mit dem Albtraum:
„Sicherheitsvorfall in geschäftskritischer Microsoft Exchange Infrastruktur“

Protokoll- und clientaffine Sicherheitsarchitektur für Microsoft Exchange.
Alle Architekturen, onPremises oder Hybrid – wir schützen Sie nachhaltig und dauerhaft!

www.braincon.de / info@braincon.de

DSGVO IT-CONSULTING MADE IN GERMANY

# Das Problem:

Bis heute herrscht ein subjektives Sicherheitsgefühl beim Betrieb von Exchange Server Infrastrukturen auf Basis geltender Best Practices und Vorgaben gemäß des bekannten Microsoft Implementierungsleitfadens.
Darüber hinaus gehende Schutzmaßnahmen gelten als kompliziert, cloud-inkompatibel und gehen einher mit einem erklärungsbedürftigen Preis-/Leistungsverhältnis. Warum also mehr aufwenden? Der jüngste Angriff der HAFNIUM-Gruppe aus dem März 2021 (CVE-2021-26855 u.a.) setzt diese Annahme außer Kraft.

# Die Herausforderung:

Wie funktioniert „Exchange Server" eigentlich im Zusammenhang mit notwendigen Zugriffen aus öffentlichen Netzen, sowohl seitens der Microsoft 365 Backplane (für hybride Bereitstellung), als auch im Kontext realer Clients, wie Windows 10 Outlook Anywhere, Outlook Apps auf SmartPhones, ActiveSync mit und ohne MDM/Intune-Szenario, Autodiscover, Teams-Integration, und vielem mehr?
Dieses Expertenthema ist durch die Implementierungsleitfäden nur sehr oberflächlich erschlossen. Eine eindeutige „Freund/Feind-Unterscheidung" im Perimeter ist in diesem Zusammenhang in den letzten 5 Jahren deutlich schwieriger geworden.
Wie aktuelle Bedrohungseinschätzungen, z.B. des BSI bekräftigen, schließen bekannte Industriestandardprodukte diese Lücke nur unzureichend.

braincon

# Unser Angebot:

Wir beschäftigen uns mit dem Schutz von Webservices seit über 10 Jahren sehr erfolgreich und mit hohem Sachverstand in Bezug auf die eingesetzten Applikations-produkte. *Exchange ist auch nur eine Webapplikation!* Selbst im hybriden Modell verbleibt eine reale onPremises-Gefahr, völlig unabhängig von der Anzahl der o365-Postfächer. Unsere aktiven Installationen hielten bislang jeder Exploit-Situation stand, auch ohne sofortiges Einspielen der entsprechenden Hotfixes. Unser Konzept berücksichtigt sowohl die Aspekte der „Positivdefinition", als auch Authentisierungskonzepte für Cloud und Legacy-Clients.

Mit unserem Lösungskatalog zeigen wir für jede Exchange Server Situation die offensichtlichen Schwachstellen auf und helfen Ihnen mit einem Maßnahmenkatalog, der Produktintegration und -konfiguration sowie Managed Services Konzepten weiter. So meistern Sie aktuelle und künftige Bedrohungssituationen erfolgreich.

# Agenda für unseren KickOff Workshop:

- Besprechung der aktuellen Exchange-Architektur
- Analyse der vorhandenen Sicherheitskonzepte
- Definition der Zugriffsrollen und -clients
- Schwachstellendiskussion
- Mögliche HighLevel-Architektur
- Vorschlag zum Betriebskonzept für (neue) Funktionen und Technologien aus unserem erprobten und betriebsfertigen Baukastensystem

## Kontaktieren Sie uns unter 06106 / 669 7 - 100