Folgend finden Sie Hintergründe und wichtige Hinweise zum Umgang mit den Sicherheitslücken.

Was ist passiert?

Am 11. Juni gab Microsoft bekannt, dass die kriminelle Hackergruppe Storm-0558 in den Besitz eines Signaturschlüssels von Microsoft gekommen war. Mithilfe dieses Schlüssels hatten die Angreifer die Möglichkeit, funktionierende Zugangstoken für Outlook Web Access (OWA) und Outlook.com zu deaktivieren und über verschiedene Skripte u.a. E-Mails und deren Anhänge herunterzuladen. Nach Angaben der Sicherheitsfirma Wiz bietet der Schlüssel darüber hinaus die Möglichkeit, sich Zugriff auf alle Microsoft-Cloud-Anwendungen, u.a. Sharepoint oder Teams, zu verschaffen. Bisher ist unklar, wie die Bedrohungsaktuere den Schlüssel erlangen konnten bzw. ob und in welchem Umfang Zugänge zu der Microsoft 365-Infrastruktur damit ausgenutzt wurden.

Wer ist betroffen?

Es wurde bekannt, dass sich die Hackergruppe Zugriff auf Online-Exchange-Konten verschiedener Regierungsbehörden verschaffte. Aufmerksam auf die Vorfälle wurde nicht der Hersteller selbst, sondern seine Nutzenden. Über die Funktion "Premium-Log-Daten" bemerkten und meldeten sie verdächtige Aktivitäten. Nach Angaben von Microsoft läuft der Angriff bereits seit dem 15. Mai 2023.

Warum ist der Vorfall so gravierend?

Dieser Vorfall unterstreicht mehrere Sicherheitslücken in Microsoft 365. So gelang es den Angreifern beispielsweise, einen Signaturschlüssel zu stehlen, der es ihnen ermöglichte, Zugriffstokens zu generieren und sich unbemerkt Zugang zu Exchange-Online-Konten zu verschaffen. Der Schlüssel war ursprünglich nicht dafür vorgesehen, auch gültige Zugriffstoken für den Business-Bereich von Azure AD (Active Directory), dem cloudbasierten Dienst zur Identitäts- und Zugriffsverwaltung, auszustellen - er funktionierte dennoch. Daher ist ungewiss, in welchem Ausmaß die Angreifer mittels des gestohlenen Schlüssel Zugriff auf die gesamte Microsoft 365-Infrastruktur hatten. Dies stellt ein gravierendes Sicherheitsrisiko für die Microsoft-Anwendungen dar.

Was kann ich tun?

Nach Angaben von Microsoft wurde die akute Bedrohung auf die Dienste Exchange Online und Outlook.com entschärft. Es seien keinerlei Maßnahmen von Seiten der Nutzenden erforderlich. Aufgrund der Tatsache, dass das Gesamtausmaß des entwendeten Schlüssels auf alle

cloudbasierten Microsoft-Anwendungen unbekannt ist, empfehlen unsere Cybersicherheitsexperten untenstehende Handlungsschritte zu befolgen:

Als Reaktion auf diese Sicherheitsverletzung sagte Microsoft zu, seinen Nutzenden umfangreicheren Einblick in seine Systeme zu gewähren. Es wurde bekannt gegeben, dass der bisherige Ansatz, den Nutzenden von Microsoft 365 nur begrenzte Protokollierungsdaten zur Verfügung zu stellen, verworfen würde. Stattdessen erhielten alle Microsoft 365 Kunden ab September kostenlosen Zugang zu umfangreichen Protokolldaten (aktuell bekannt als PurView Premium).

- **Aktivieren Sie die PurView Audit (Premium)-Protokollierung:** Diese Protokollierung erfordert eine Lizenzierung auf der G5/E5 Ebene. Weitere Informationen finden Sie in der Anleitung von Microsoft zur Zuweisung von Microsoft 365-Lizenzen an Benutzer.

- **Stellen Sie sicher, dass die Protokolle für Administratoren durchsuchbar sind**: Die relevanten Protokolle müssen für Administratoren oder Forensiker des Unternehmens zugänglich sein, um zu untersuchen, ob Anomalien in den Protokollen gefunden werden können.

- **Aktivieren Sie Microsoft 365 Unified Audit Logging (UAL):** UAL sollte standardmäßig aktiviert sein, aber es wird empfohlen, diese Einstellungen zu validieren.

- **Verstehen Sie die Cloud-Logs Ihres Unternehmens:** Unternehmen sollten sich mit den Standard-Protokollen, die ihre Cloud generiert, auseinandersetzen, um ungewöhnlichen und normalen Datenverkehr besser verstehen und differenzieren zu können.

Im Fall eines Abflusses von Zugangsdaten (kein MFA): Informieren Sie innerhalb von 72h die zuständige Landesdatenschutzbehörde, dass ein Angreifer Zugriff auf Benutzerdaten hatte. Aus den Logs von M365 ist derzeit nicht erkennbar, ob z.B. eine vollständige Synchronisation erfolgt ist.