Q&A: Ransomware-Vorfall Xplain

Durch den Ransomware-Angriff auf das Unternehmen Xplain, bei dem ein Teil der entwendeten Daten im Darknet publiziert wurde, könnten nach aktuellem Kenntnisstand auch operative Daten der Bundesverwaltung betroffen sein. Die vertieften Analysen laufen derzeit noch.

Datum: 09.06.2023

Inhalt

1. Welche Verwaltungseinheiten in der Bundesverwaltung sind betroffen?

Welche Bundesstellen betroffen sind, ist Bestandteil der laufenden Analyse.

2. Stehen der Angriff auf Xplain und der Angriff auf die Parlamentsdienste in einem Zusammenhang?

Nein, es sind zwei verschiedene Vorkommnisse, die nicht zusammenhängen. Es stehen auch verschiedene Gruppierungen hinter den Angriffen. So steht hinter dem Angriff auf Xplain die Gruppe «Play» und zum DDoS-Angriff auf die Parlamentsdienst-Webseite hat sich auf Telegramm die Gruppe «NoName» bekannt.

3. Wurde Lösegeld bezahlt?

Das NCSC wurde informiert, dass kein Lösegeld bezahlt wurde.

4. Was für Daten sind betroffen?

Entgegen erster Erkenntnisse muss nach aktuellen vertieften Abklärungen davon ausgegangen werden, dass auch operative Daten betroffen sein könnten. Operative Daten sind solche, die dienstlich genutzt werden. Die Analyse der Daten dauert an, daher können wir keine konkreteren Angaben machen.

5. Konnten die Angreifer auf die Bundessysteme zugreifen?

Bislang konnte kein Zugriffsversuch auf Bundessysteme beobachtet werden.

6. Warum übernimmt das NCSC erst jetzt die Koordination?

Das NCSC hat Xplain direkt nach Meldung des Vorfalls seine Unterstützung angeboten. Mit dem Bekanntwerden der Tragweite hat das NCSC die Führung und Koordination gemäss seinem Auftrag übernommen.
Die Zuständigkeiten sind im Rahmen der Art. 12, Abs 5 & 6 CyRVv (Cyberrisikenverordnung) geregelt.

7. Was wissen Sie über die Hackergruppe «Play»?

Das NCSC kann den öffentlich verfügbaren Informationen nichts hinzufügen.

8. Was sind die nächsten Schritte?

Aktuell werden die publizierten Daten analysiert. Die Erkenntnisse werden mit den betroffenen Verwaltungseinheiten besprochen und weitere Massnahmen definiert.

9. Wer ist an den Analysen beteiligt?

Es sind verschiedene Stellen der Bundesverwaltung sowie die Strafverfolgungsbehörden an der Analyse des Vorfalles beteiligt. Aufgrund des aktuell laufenden Strafverfahrens können hierzu keine konkreteren Angaben gemacht werden.

10. Inwiefern ist es problematisch, dass verschiedene Bundestellen beim selben IT-Dienstleister angeschlossen sind?

Dass verschiedene Bundesstellen teilweise die gleichen IT-Dienstleister benutzen ist nicht per se problematisch. Einem gewissen Klumpenrisiko steht eine bessere Wirtschaftlichkeit gegenüber.
Weiter muss beachtet werden, dass es oftmals nicht unzählige Firmen gibt, die die geforderte Leistung erbringen können.

Abschliessend ist anzumerken, dass das Nutzen mehrerer Lieferanten auch zu zusätzlichen Schnittstellen und Datenaustauschen führt, was wiederum das Risiko eines Sicherheitsvorfalls erhöhen kann.

11. Wie läuft ein Ransomware-Angriff ab?

Nachdem die Angreifer sich unbefugten Zugriff auf die Systeme einer Unternehmung verschafft haben, werden die Daten zuerst gestohlen, danach verschlüsselt und die Firma wird erpresst. Zahlt die betroffene Firma nicht, wird mit der Veröffentlichung der gestohlenen Daten gedroht. Tritt die Firma auf die Erpressung weiterhin nicht ein, so werden die Daten meistens schrittweise veröffentlicht um den Druck stetig zu erhöhen.

12. Stellen Sie fest, dass die Cyberkriminalität zunimmt?

Das Thema Cybersicherheit ist in den letzten Jahren in allen Bereichen verstärkt in den Fokus gerückt. Dies, sowie die verstärke Berichterstattung in den Medien führte dazu, dass viele Unternehmen, die heute Opfer eines Cyberangriffs geworden sind, eher an die Öffentlichkeit gehen. Jedoch nimmt das NCSC auch eine leichte Steigerung der Cybervorfälle war.

13. Gibt es vermehrt Ransomware-Angriffe?

Die Meldungen zu Ransomware-Angriffen sind von 2020-2021 stark gestiegen und haben sich nun auf diesem Niveau eingependelt. Allerdings sind in diesem Jahr prozentual mehr Firmen und weniger Privatpersonen betroffen als in den beiden Jahren zuvor. Während der Anteil von Meldungen ans NCSC zu Ransomware-Angriffen von Privatpersonen 2021 und 2022 etwa 35% betrug, sind es 2023 nur noch etwa 10%. Die Angreifer scheinen sich mehr auf Unternehmen zu fokussieren. Das Einfallstor bei Ransomware-Angriffen geht meist auf ungepatchte Systeme oder der Missbrauch von Zugangsdaten zurück.

<u>Anzahl Meldungen zu Ransomware-Angriffen:</u>

2020: 66 Meldungen
2021: 161 Meldungen
2022: 159 Meldungen
2023: 56 Meldungen (05.06.2023)

<u>Anzahl Meldungen zu Cybervorfällen insgesamt:</u>

2020 10'833 Meldungen
2021 21'714 Meldungen
2022 34'527 Meldungen

2023 15'977 Meldungen (Stand 05.06.2023)

Zu beachten ist, dass in der Schweiz keine generelle Meldepflicht für Cybervorfälle besteht. Deshalb kann davon ausgegangen werden, dass die Dunkelziffer entsprechend höher ist.

14. Wie kann sich ein Unternehmen vor Ransomware schützen?

Mit den richtigen Schutzmassnahmen lässt sich das Risiko von einem erfolgreichen Cyberangriff stark minimieren. Aus diesem Grund warnt das NCSC immer wieder vor den erhöhten Sicherheitsrisiken durch Ransomware. Dennoch setzen viele Schweizer Unternehmen diese nicht oder nur teilweise um. Dies führt nicht nur zu einer sehr hohen Risikoexposition der Unternehmen, sondern auch dazu, dass immer wieder Schweizer Unternehmen Opfer von Ransomware werden und deren Daten aber auch solche von Mitarbeitenden oder Kunden im Internet veröffentlicht werden.

Absicherung von Fernzugängen:
Alle Fernzugänge wie VPN, RDP, Citrix, usw. sowie sämtliche andere Zugänge auf interne Ressourcen (z. B. Webmail, Sharepoint, usw.) müssen zwingend und konsequent mit einem zweiten Faktor abgesichert werden (Zwei-Faktor-Authentisierung – 2FA). Dies gilt auch für Zugänge von Beispielsweise Lieferanten, Vertragspartnern oder Student/innen.

Patch- und Lifecycle-Management:
Sämtliche Systeme müssen konsequent und zeitnah mit Sicherheitsaktualisierungen (Updates) versorgt werden. Updates, welche kritische Sicherheitslücken in über das Internet erreichbare Systeme beheben, müssen innerhalb 24 Stunden eingespielt werden. Software oder Systeme, welche vom Hersteller nicht mehr unterstützt werden («End of Life» - EOL) müssen abgeschaltet oder in eine separate, abgeschottete Netzzone verlegt werden.

Offline-Backups:
Erstellen Sie regelmässig Sicherungskopien (Backups) Ihrer Daten. Nutzen Sie dabei das Generationenprinzip (täglich, wöchentlich, monatlich - mindestens 2 Generationen). Stellen Sie jeweils sicher, dass Sie das Medium, auf welchem Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer bzw. Netzwerk physisch trennen und sicher aufbewahren oder verwenden Sie WORM-Speichermedien.

Weiterführende Informationen:

Ransomware-Banden sind weiterhin sehr aktiv in der Schweiz (admin.ch)