Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Melde- und Analysestelle Informationssicherung MELANI

Vorsicht: Weiterhin erhöhtes Sicherheitsrisiko durch Ransomware gegen KMUs

19.02.2020 - In den vergangenen Wochen hat MELANI / GovCERT mehr als ein Dutzend Ransomware-Fälle bearbeitet, bei welchen unbekannte Täter die Systeme von Schweizer KMUs und Grossbetrieben verschlüsselt und damit unbrauchbar gemacht haben. Die Angreifer stellten Lösegeldforderungen von mehreren zehntausend Franken, vereinzelt auch von Millionenbeträgen.

Bei der technischen Analyse der Vorfälle hat sich gezeigt, dass die IT-Sicherheit der betroffenen Unternehmen oftmals lückenhaft war und die üblichen «best-practices» (Merkblatt Informationssicherheit für KMUs) nicht vollständig eingehalten wurden. Zudem wurden auch Warnmeldungen von Behörden nicht beachtet.

Bei der Aufarbeitung der Vorfälle der letzten Wochen haben sich insbesondere untenstehende Schwachstellen als Einfallstor für die Cyberangriffe herauskristallisiert die durch die Umsetzung der MELANI-Empfehlungen geschlossen werden können.:

1. Virenschutz und Warnmeldungen
Warnmeldungen von Antivirensoftware, dass auf Servern (z. B. Domain-Controllern) Malware gefunden wurde, wurden von den Unternehmen entweder nicht bemerkt oder nicht ernst genommen. In wenigen Fällen war auf einigen Servern sogar überhaupt keine Antivirensoftware installiert. Dies kann massgeblich zur Ausbreitung von Malware innerhalb von Unternehmensnetzwerken beitragen.

Empfehlungen:
• Antiviren-Software muss flächendeckend auf allen Clients und Servern eingesetzt werden.

• **Warnmeldungen von Antiviren-Software müssen geloggt und regelmässig überprüft werden.** Sollte eine vollständige Prüfung der Warnmeldungen nicht möglich sein (z. B. aufgrund der hohen Anzahl), sollten mindestens solche von Servern (z. B. Domain-Controllern, Backup, usw.) täglich geprüft werden.

2. Schutz der Fernzugriffe («Remote-Zugriffe»)
Oftmals waren Fernzugriffe auf Systeme, sogenannte Remote Zugänge (Remote Desktop Protocol – RDP), nur mit einem schwachen Passwort geschützt und der Eingang nur standardmässig eingestellt (Standardport 3389), ohne Einschränkung (z. B. VPN oder IP-Filter). Dadurch waren die Systeme sehr leicht zugänglich. Die Angreifer konnten auf einfache Weise unbemerkt in Unternehmensnetzwerke eindringen und Malware installieren.

Empfehlung:
• **Sämtliche Fernzugänge wie z. B. VPN und RDP (Terminalserver) müssen mittels Zwei-Faktor-Authentisierung abgesichert werden.** Zusätzlich sollten diese, wenn immer möglich, nicht auf Standardports (z. B. 3389 für RDP) horchen. Der Einsatz und das Durchsetzen einer Passwortrichtline zur Verhinderung einfacher Passwörter («123456», « password», usw.) ist dabei unabdingbar.

3. Behördenmeldungen
Meldungen von Behörden oder von Internet Service Providern (ISPs) über allfällige Infektionen wurden von den betroffenen Unternehmen ignoriert oder nicht ernstgenommen. Infektionen wurden somit nur teilweise oder gar nicht bereinigt, was in vielen Fällen zu einer kompletten Verschlüsselung des Unternehmensnetzwerkes führte.

Empfehlung:
• **Meldungen von Behörden und Internet Service Providern (ISPs) betreffend Infektionen müssen ernst genommen werden.** Im Zweifelsfalle (z. B. Authentizität einer Meldung) wenden Sie sich an die absendende Behörde oder den Provider.

4. Offline-Backups und Updates
Viele Unternehmen verfügten nur über Online-Backups, welche nicht vom System abgekoppelt (offline) zur Verfügung stehen. Bei einem Befall mit Ransomware wurden diese somit ebenfalls entweder verschlüsselt oder unwiderruflich gelöscht. Eine Wiederherstellung der Unternehmenstätigkeit war dadurch in vielen Fällen nur mit erheblichem Aufwand oder überhaupt nicht mehr möglich.

Empfehlungen:

• **Erstellen Sie regelmässig eine Sicherungskopie (Backup) Ihrer Daten.** Die Sicherungskopie muss offline (z. B auf einem externen Medium wie beispielsweise einer externen Festplatte oder einem Backup-Tape) gespeichert werden. **Stellen Sie sicher, dass Sie das Medium, auf welchem Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang physisch vom Computer bzw. Netzwerk trennen.** Definieren Sie zudem einen Prozess, der die regelmässige Datensicherung festlegt und halten Sie diesen konsequent ein.

• **Sorgen Sie für konsequente Updates.** Sowohl Betriebssysteme als auch alle auf den Computern und Servern installierten Software (z. B. Adobe Reader, Adobe Flash, Oracle Java usw.) müssen konsequent auf den neuesten Stand gebracht werden. Falls möglich, am besten mit der automatischen Update-Funktion vornehmen.

5. Patch- und Lifecycle-Management

Oftmals führen Unternehmen kein sauberes Patch- und Life-Cycle Management. Dadurch waren veraltete, nicht mehr unterstützte Betriebssysteme oder Software im Einsatz. Die Angreifer nutzten die Sicherheitslücken aus und verschafften sich dadurch Zugang zum Unternehmensnetzwerk und weiteren internen Systemen. Hat sich ein Angreifer Zugang zum Netzwerk verschafft, begünstigt ein mangelhaftes Patch- und Life-Cycle Management zudem die Weiterverbreitung der Malware innerhalb des Netzwerkes.

Empfehlungen:

• **Führen Sie ein Patch- und Life-Cycle Management.**
Trennen Sie veraltete Systeme vom Netzwerk, wenn Sie diese nicht mehr benötigen oder ersetzen Sie diese so rasch wie möglich.

• **Isolieren Sie schlecht geschützte Systeme.** Sollten Systeme mit einem alten Betriebssystem (z. B. Windows XP, Windows 2003 Server, Windows 2008 Server) vorhanden sein, die nicht migriert werden können, müssen diese zwingend so weit wie möglich isoliert werden. Es sollten nur diejenigen Verbindungen vom und zum System erlaubt werden, welche für den reibungslosen Betrieb unabdingbar sind.

6. Keine Segmentierung

Die Netzwerke waren nicht aufgeteilt (segmentiert), d. h. dass eine Infektion z. B. auf einem Rechner der Personalabteilung dem Angreifer einen direkten Angriffspfad in die Produktionsabteilung ermöglichte.

Empfehlung:
• Netzwerke sollten zumindest minimal segmentiert werden, so dass kritische Umgebungen abgeschottet sind.

7. Zu hohe Benutzerrechte
Häufig wurden Benutzer mit zu hohen Rechten ausgestattet, z. B. ein Backup User, der Domain Admin Rechte hat oder der Systemverantwortliche, der mit denselben Rechten sowohl im Internet surft wie er die Systeme verwaltet.

Empfehlung:
• Definieren Sie in einem **Rollenkonzept**, für welche Art von Benutzern welche Rechte notwendig sind. Stellen Sie ausserdem sicher, dass die Rechte bei personellen Wechseln (Verlassen der Firma, Wechsel in eine andere Abteilung) entsprechend angepasst werden können.

Vorsicht bei Lösegeldforderungen
Wurden Systeme durch eine Ransomware verschlüsselt, rät MELANI von einer Lösegeldzahlung ab. Grundsätzlich empfiehlt MELANI nicht zu bezahlen, weil dadurch die Infrastruktur der Hacker unterstützt wird. Zudem muss beachtet werden, dass es auch bei der Bezahlung von Lösegeld keine Garantie gibt, dass der Erpresser die Daten wieder entschlüsselt.
Wichtig ist, dass die betroffenen Unternehmen unverzüglich mit der Kantonspolizei Kontakt aufnehmen, Anzeige erstatten und mit Ihnen das weitere Vorgehen besprechen.
Solange es weiterhin Unternehmen gibt, welche Lösegeld bezahlen, werden die Angreifer nie mit den Erpressungen aufhören.

Wird dennoch eine Lösegeldzahlung in Erwägung gezogen ist zu beachten, dass Systeme und Daten zwar entschlüsselt werden könnten, die zugrundeliegende Infektion durch Malware wie «Emotet» oder «TrickBot» bleibt jedoch weiterhin aktiv. Infolgedessen haben die Angreifer weiterhin vollen Zugriff auf das Netzwerk des betroffenen Unternehmens und können beispielsweise erneut Ransomware installieren oder sensible Daten aus dem Unternehmensnetzwerk stehlen. So sind MELANI Fälle im In- und Ausland bekannt, wo dieselben Unternehmen innert kürzester Zeit mehrmals Opfer von Ransomware wurden.

Eigenverantwortung wahrnehmen
MELANI hat bereits im vergangenen Jahr zusammen mit Partnern im Rahmen des Private-Public-Partnership (PPP) Massnahmen getroffen, um die Bedrohung durch einzelne Akteure sowie die Verbreitung von Malware in der Schweiz zu reduzieren. Grundsätzlich appelliert MELANI jedoch einmal mehr an die

Wahrnehmung der Eigenverantwortung aller Schweizer Unternehmen betreffend sicherem Betrieb ihrer IT-Infrastruktur.

✉ Fachkontakt

Letzte Änderung 19.02.2020

https://www.melani.admin.ch/content/melani/de/home/dokumentation/newsletter/sicherheitsris durch-ransomware.html