BVSW

LEITFADEN

CYBERANGRIFF

BVSW

BVSW DIGITAL

ASW

Bundesverband

Allgemeine Verhaltensweisen:

RUHE BEWAHREN
Cyberkriminelle setzen ihre Opfer gezielt unter Zeitdruck. Bleiben Sie ruhig und handeln Sie überlegt. Lassen Sie sich nicht zur Installation von Software verleiten, die angeblich den Entschlüsselungscode liefern soll.

SCHNELL REAGIEREN
Verlieren Sie keine Zeit. Starten Sie so schnell wie möglich die folgenden Schritte, die wir in diesem Leitfaden präsentieren.

INHALT

1 TECHNISCHE SOFORTMASSNAHMEN

Auf keinen Fall mit Admin-Konten auf den Systemen anmelden

Nicht mehr an den Geräten arbeiten

Backups schützen, indem sie vom Netzwerk und Geräten getrennt werden

A Notfallmaßnahmen am Gerät

Schalten Sie das Gerät nicht aus, sondern trennen Sie sämtliche Netzwerk- und Kommunikationsverbindungen, um eine weitere Ausbreitung im Netzwerk zu unterbinden.

Dafür haben Sie zwei Möglichkeiten:

- Über das Gerät selbst. Fahren Sie das Gerät nicht herunter, sondern ziehen Sie das LAN-Kabel ab, deaktivieren Sie die WLAN-Verbindung und Bluetooth
- Über die entsprechenden Ports am Netzwerk-Switch

B Notfallmaßnahmen am Netzwerk

- Trennen aller Netzwerkverbindungen des Unternehmens nach außen (Firewall, Internet)
- Client-Remote-Zugänge abschalten
- Funknetze abschalten (WLAN, 5G Netz)

- IT-Endgeräte vom Netzwerk trennen – ACHTUNG: Fast alle modernen elektrischen Geräte haben eine Internetschnittstelle (Drucker, Server, Notebooks, PCs, Smart-TV, Präsentationsgeräte, Kaffeemaschine...)
- Interne Router und Switches abschalten (Router in das Produktionsnetz, Stockwerk-Switch, etc.)

2 KRISENSTAB EINRICHTEN

Richten Sie einen Krisenstab ein, der alle Informationen zusammenführt und durch die Krise navigiert. Folgende interne Stellen sollten am Krisenstab beteiligt sein:

- Leitungsebene, aber nicht der Kopf des Unternehmens (Gefahr der Überlastung)
- IT-Leitung (Technischer Sachverstand)
  Juristen (Klärung Haftung, Strafanzeige)
- Presse- und Öffentlichkeitsarbeit als einzige Stelle, die nach Außen kommuniziert
- Datenschutzbeauftragte
  (Datenschutzrechtliche Fragen, z.B. Logging)
- Personal-/Betriebsrat

Für den Notbetrieb finden sich womöglich noch wichtige Daten bei Außenstellen oder auf Systemen von Mitarbeitern, die aktuell im Urlaub sind.

3 MELDEPFLICHTEN BEACHTEN

Wer von einer Cyberattacke betroffen ist, hat bestimmte Meldepflichten zu beachten. Folgende Stellen, bzw. Personen müssen benachrichtigt werden:

- **Landesdatenschutzbeauftragte:** Sind bei einer Cyberattacke personenbezogene Daten abgeflossen, so MUSS nach DSGVO (Art. 33. DSGVO) innerhalb von 72 Stunden die zuständige Aufsichtsbehörde, der Landesdatenschutzbeauftragte, benachrichtigt werden.
- **Betroffene Personen:** Direkt betroffene Personen (Mitarbeiter, Kunden, Newsletter-Empfänger, ...), deren Daten abgeflossen sind, müssen ebenso benachrichtigt werden. Erklären Sie, welche Daten abhandengekommen sind und wie hoch das Missbrauchspotential ist. Informieren Sie außerdem über die eigenen ergriffenen Schutzmaßnahmen.
- **BSI:** Betreiber kritischer Infrastrukturen müssen eine Datenpanne an das Bundesamt für Sicherheit in der Informationstechnik melden.
- **Vertragspartner:** Aus Verträgen ergeben sich eventuell auch Meldepflichten gegenüber den Vertragspartnern.
- **Cyber-Versicherung:** Sollte Ihr Unternehmen über eine Cyber-Versicherung verfügen, informieren Sie diese umgehend. Auch hier gibt es häufig Vorgaben über das notwendige Vorgehen.

4 EXTERNE UNTERSTÜTZUNG

Wenden Sie sich frühzeitig an externe Experten, wenn Sie sich überfordert fühlen. Helfen können verschiedene Institutionen:

BSI

Bei besonders schweren IT-Sicherheitsvorfällen ist das Bundesamt für Sicherheit in der Informationstechnik kompetenter Ansprechpartner. Die Vorfälle müssen dabei von besonderer technischer Qualität und die Wiederherstellung der Systeme von herausragendem öffentlichem Interesse sein. Anders als die Polizei kümmert sich das BSI nicht um die Strafverfolgung.

IT-Dienstleister

IT-Dienstleister haben unterschiedliche Schwerpunkte. Beschreiben Sie bei der Kontaktaufnahme möglichst genau, welche Unterstützung Sie benötigen. (Bereinigen des Systems, Wiederaufbau des Netzwerks, etc.) Auf der Website des BSI findet sich eine Liste qualifizierter ATP-Response-Dienstleister.

Verbände, BVSW

Verbände haben ein starkes Netzwerk aus unterschiedlichsten Sicherheitsexperten. Neben IT-Experten finden sich hier auch erfahrene Verhandlungsprofis für die Kontaktaufnahme mit IT-Kriminellen. Außerdem halten sie einen engen Kontakt zu den Sicherheitsbehörden.

Polizei

Cybercrime ist eine Straftat, deren Aufklärung und Ahndung der Polizei obliegt.

Das Bundeskriminalamt sowie die jeweiligen Landeskriminalämter haben deshalb spezialisierte Anlaufstellen eingerichtet.

Die Zentrale Ansprechstelle Cybercrime (ZAC) steht den Opfern zur Seite, wenn es um die Beweissicherung und die Erstattung einer Anzeige geht.

Wenn Sie mit der Polizei Kontakt aufnehmen, sprechen Sie im Konjunktiv. („Angenommen, meine Firma wäre von einem Cybervorfall betroffen...“) Sobald die Polizei von einer Cyberattacke erfährt, muss sie ermitteln (Legalitätsprinzip).

5 VORFALL BESCHREIBEN

Für die Wiederherstellung der Systeme sowie für die Strafverfolgung muss genau dokumentiert werden, was vorgefallen ist. Je mehr Beweise Sie sichern können, desto mehr Anhaltspunkte ergeben sich für die IT-Dienstleister sowie für die Strafverfolgungsbehörden.

Klären Sie folgende Fragen soweit möglich:

1. **Was genau ist passiert? (Der Rechner wurde langsam, der Bildschirm wurde blau, ...)**
2. **Welche Geräte oder Systeme sind betroffen? Wie lauten der Hersteller und das Modell?**
3. **Woran haben Sie gearbeitet, als der Vorfall eintraf? Welche Programme und welche Dokumente waren geöffnet?**
4. **Wann ist es passiert?**

6 LÖSEGELD – ZAHLEN ODER NICHT?

Bei Ransomware-Attacken werden Daten verschlüsselt und die Täter fordern ein Lösegeld für die Übersendung eines Entschlüsselungs-Codes. Bei der Entscheidung, ob Sie auf die Forderung eingehen wollen oder nicht, sollten Sie beachten:

Verhandeln Sie niemals direkt mit den Erpressern!

- Sollten Sie eine Zahlung in Erwägung ziehen, lassen Sie einen erfahrenen Verhandlungsprofi mit den Erpressern Kontakt aufnehmen. Auch wenn Sie im alltäglichen Geschäftsleben ein begnadeter Verhandler sind – hier geht es um Verhandlungen mit Kriminellen.
- Bei Zahlung landen Sie bei den Erpressern womöglich auf der Liste für „gute Kunden“ und geraten damit in den Fokus weiterer Erpressungen und neuer Tätergruppen.
- Trotz Zahlung haben Sie keine Garantie, dass alle Daten wieder entschlüsselt werden.
- Polizei und BSI raten grundsätzlich von einer Lösegeldzahlung ab, weil dies eine Finanzierung krimineller Aktivitäten darstellt. Zahlungen und ihre Konsequenzen sollten deshalb mit Ihrer Rechtsabteilung oder Rechtsanwälten sowie den zuständigen Ermittlungsbehörden abgeklärt werden.
- Eine erfolgreiche Entschlüsselung ersetzt keinesfalls die Neuinstallation der kompromittierten Systeme. Die Täter könnten eine Hintertür hinterlassen haben, über die es zu einer erneuten Verschlüsselung kommen kann.

7 BEWEISE SICHERN

<u>Wichtig:</u> Das infizierte System sollte so wenig wie möglich angefasst werden

Damit der Umfang und die Art des Angriffs besser eingeschätzt werden können, ist eine digitale Beweisaufnahme erforderlich. Wenn Sie die notwendigen Kompetenzen dafür nicht im Haus haben, überlassen Sie die Beweissicherung unbedingt einem IT-Experten. Unsachgemäß durchgeführte Analysen auf einem kompromittierten System könnten dazu führen, dass ermittlungsrelevante Dateien zerstört oder gelöscht werden. Folgende Sicherungsmaßnahmen sind erforderlich:

- **Bei eingeschalteten Systemen:**
  Erstellung eines forensischen Abbildes des Arbeitsspeichers.
- **Festplattenimage:**
  Erstellung eines forensischen Images (1:1 Sektorkopie). Über marktübliche Festplatten-Backup-Programme ist das in der Regel nicht möglich.
- **Virtuelle Systeme:**
  Verzeichnis der Virtualisierungssoftware sichern.

8 WIEDERHERSTELLUNG

Schadprogramme nehmen tiefgreifende Änderungen am infizierten System vor. Deshalb sollten kompromittierte Systeme vollständig neu aufgesetzt werden. Neben der Neuinstallation gibt es zu beachten:

1. **Angriffskette und Infektionsvektor identifizieren**
2. **Neue Log-in Daten und Passwörter für alle Nutzer erstellen**
3. **Eventuell 2-Faktor-Authentifizierung einführen**
4. **Langfristig das Active Directory (AD) neu aufsetzen**

►►► Übersicht-Tafel zum Ausdrucken und an die Wand hängen ►►►

LEITFADEN CYBERANGRIFF

– wie verhalte ich mich im Ernstfall?

Ruhe bewahren schnell handeln

1. Geräte vom Netzwerk trennen: Netzwerkstecker ziehen / W-Lan ausschalten
2. Krisenstab alarmieren
3. Gesetzliche Meldepflichten beachten
4. Externe Unterstützung suchen
5. Vorfall detailliert beschreiben
6. Lösegeld: Entscheidung treffen
7. Beweise sichern
8. System wiederherstellen

www.bvsw.de

BAYERISCHER VERBAND FÜR SICHERHEIT IN DER WIRTSCHAFT E. V.

BVSW