Incident-Response-Playbook

Empfehlungen Secutec

Secutec
Cybersecurity Intelligence

Inhaltsverzeichnis

1 Nach der Cyberattacke

2 Ausbruchsphase

2.1.1 Kontaktieren Sie das Management, Ihren IT-Dienstleister, Ihre Cyberversicherung und/oder Secutec für die Unterstützung.

Hotline: +00 0000 00000

2.1.2 Internetverbindungen

a. Trennen Sie alle Ihre Internetverbindungen – eingehend und ausgehend
b. Wenn Sie zusätzliche Wi-Fi Internetverbindungen bereitstellen, trennen Sie auch alle diese Verbindungen.
c. Gehen Sie zunächst davon aus, dass jedes Gerät infiziert ist. (auch auf die internen Kommunikationsmittel achten, diese könnten von Cyberkriminellen mitgelesen werden).
d. Techniker benötigen ein Internet, erstellen Sie dazu einen Hotspott (4G-WLAN + saubere Laptops/Workstations).
e. Wenden Sie sich an Ihren IT-Dienstleister, um Sie zu unterstützen.

2.1.3 Backups

a. Sichern Sie Ihre Offsite-/Onsite-Backup- Systeme
b. Trennen Sie die Backup Storage vom Netzwerk oder sperren Sie den Zugang zu den Backup Systeme.

2.1.4 Inventar

a. Überprüfen Sie den Status der Backups
b. Ermitteln Sie, welche Systeme betroffen waren, und isolieren Sie diese vom Netzwerk
c. Infizierte Geräte NICHT herunterfahren!
d. Trennen Sie die Backup Storage vom Netzwerk oder sperren Sie den Zugang zu den Backup Systemen.
e. Trennen Sie die Backup Storage vom Netzwerk oder sperren Sie den Zugang zu den Backup Systemen.
f. Starten Sie keine Systeme, die bei der Attacke ausgeschaltet waren und nicht infiziert sind.

2.1.5 Netzwerk

a. Wenn Sie nicht in der Lage sind, schnell zwischen infizierten und nicht infizierten Systemen zu unterscheiden, sollten Sie Ihr Netzwerk abschalten, um eine weitere Ausbreitung zu verhindern.
   Vorsicht bei Rechenzentren, remote Locations ...
b. Wenn Sie ein großes Netzwerk haben, beginnen Sie damit, Domänencontroller / Produktionsserver / Entwicklungs- / Testserver zu trennen...

3 Bewertungsphase

3.1.1 Werkzeuge

a. Beginnen Sie mit der Bereitstellung von Tools auf allen Geräten (infiziert oder nicht), die die forensische Forschung unterstützen, wie secureDNS – EDR – Velociraptor (kann auch im Voraus installiert und bei Bedarf aktiviert werden). Die Installation sollte von neu installierten Servern durchgeführt und überwacht werden und in einem eigenen Netzwerk.
   Sichere Protokolle von jeder verfügbaren Quelle. Die folgenden Verbindungen müssen verfügbar sein:

   EDR:
   Stellen Sie sicher, dass die DNS-Auflösung verfügbar ist, um die richtige EDR-Instanz zu finden.
   TCP Port 443 to:
   - 35.241.219.3
   - 104.155.65.32
   - 150.136.134.49
   - 104.155.10.146

   TCP Port 80 to:
   - 104.18.11.39

Velociraptor:

Velociraptor muss über TCP-Port 443 eine Verbindung zu monitor3.secutec.be, 176.31.126.28 und 176.31.126.46 herstellen können.

Prozesse für Antivirus, wenn AV die oben genannten blockiert:

Windows-Prozesse

% ProgramFiles %**\PylumLoader.exe
% ProgramFiles %**\ActiveConsole.exe
% ProgramFiles %**\Minionhost.exe
% ProgramFiles %**\ExecutionPreventionSvc.exe
% ProgramFiles %**\CrsSvc.exe
% ProgramFiles %**\AmSvc.exe
% ProgramFiles %**\CrAmTray.exe
% ProgramFiles %**\ActiveCLIAgent.exe
% ProgramFiles %**\Wsclfsvc.exe
% ProgramFiles %**\Cybereasonsensor.exe

Fügen Sie die folgenden Pfadausschlüsse hinzu:

% ProgramData %\ apv2\Logs\
% ProgramData %\apv2\Database\
% ProgramData %\crs1 Ausführungsverhinderungsprotokolle\
% ProgramData %\crb1 Installation\
% ProgramData %\apv2\Logs Anti-Ransomware-Protokolle\
% ProgramData %\crb1\
% ProgramFiles %\ Cybereason ActiveProbe \
% ProgramFiles %\Cybereason Execution Prevention\

Installationspfade: Windows:

% ProgramFiles %\Cybereason ActiveProbe \ und
% ProgramFiles %\Cybereason Execution Prevention\

3.1.2 Server

a. Bei allen laufenden Servern, automatische Tasks deaktivieren, damit die Logdateien nicht überschrieben werden. (Security Logs, Anlegen von Admin-Usern, Access Logs, ...).
b. Logs von nicht infizierten Geräten können für die Forensik ebenfalls nützlich sein.
c. Alles kann helfen, den Patient Zero zu identifizieren!

3.1.3 Logs

a. Für die Forensik sollten möglichst viele Protokolle verfügbar gemacht werden.
   Wir empfehlen externe Log-Backups für mindestens 90 Tage.
   Hier ist eine Zusammenfassung der wichtigsten Protokolle für die Forensik:
   - Firewall Logs
   - Server Logs von verschlüsselten Servern
   - Alle anderen Logs, die helfen können (Syslogs , Monitoring Logs, ...)

3.1.4 Priorisieren

a. Überlassen Sie "dem Unternehmen", die Prioritäten auf der Grundlage der geschäftlichen Auswirkungen zu definieren - Topmanager erstellen eine Liste, die in Stein gemeißelt ist.
b. Lassen Sie dem IT-Team eine Liste mit technischen Schritten zur Erreichung der vorrangigen Geschäftsziele erstellen, abhängig von Voraussetzungen und Abhängigkeiten.

3.1.5 Netzwerk

a. Redesign des Netzwerks mit Schwerpunkt auf Segmentierung (Unterschiedliche VLANs, usw.).
b. Dieser Schritt ist zeitaufwendig und verlangsamt den Wiederaufbau, ist aber für die Zukunft von entscheidender Bedeutung.
c. Für Netzwerkkomponenten wie Firewalls und Switches: Sichern Sie die Konfiguration, bevor Sie mit der Neueinrichtung beginnen.
d. Planen Sie eine separate ausgehende Internetverbindung (green VLAN), bei der nur die erforderlichen Websites u. Ports geöffnet sind.

4 Wiederaufbauphase

4.1.1 Kommunizieren – Vertrauen

a. Wenn Sie nicht kommunizieren, werden Sie das Vertrauen Ihrer Partner/Kunden verlieren.
b. Dieses Vertrauen zu erhalten bzw. wiederherzustellen, sollte eine der obersten Prioritäten sein, um Ihr Geschäft zu erhalten.
c. Negative Nachrichten verbreiten sich rasend!
d. Übernehmen Sie die Kontrolle über die Kommunikation, um Spekulationen zu vermeiden.

4.1.2 Wiederaufbau Kommunikation

a. E-Mail (Überlegen Sie eine Migration in O365).
b. Anti-Spam-Lösung (Funktion sicherstellen).
c. Online-Webseite (Cloud Provider). Evtl. Möglichkeit einer "Dark Site" vorab prüfen.

4.1.3 Allgemeine Überlegungen

a. Verwenden Sie gängige Sicherheitsmaßnahmen. (Beispiel: AD-tiering/MFA/...).
b. Neue Hardware (sichere Hardware)
c. Netzwerk Segmentierung (red/green VLAN).
d. Folgen Sie der geschäftlichen Priorisierung.

4.1.4 Sicherheitsüberlegungen

Berücksichtigen Sie vor/während des Neuaufbaus wichtige Sicherheitsmaßnahmen, auch wenn dies den Wiederaufbau verlangsamen.

- Active Directory-Administrative-Tier-Model (unten als Beispiel)
  - *Administratorkonto Tier 0* – Zum Anmelden bei Domänencontrollern oder zur anderweitigen Verwaltung der Active Directory-Gesamtstruktur /Domäne. Betroffene Systeme: Domänencontroller, PKI, AAD Connect, Identitätsmanagementsysteme.
  - *Administratorkonto Tier 1* – Zum Anmelden bei den Anwendungsservern oder zur anderweitigen Verwaltung der in der Umgebung verwendeten Anwendungen. Betroffenes System: MSSQL, Webserver, usw.
  - *Administratorkonto Tier 2* – Zum Anmelden an der Workstation oder zur anderweitigen Verwaltung der Tier-2-Systeme, die normalerweise im Helpdesk oder Ähnlichem verwendet wird. Betroffene Systeme : Workstations, Drucker, Mobilgeräte Geräte usw.

4.1.5 Domänencontroller

a. Wiederherstellung vom Backup im red VLAN.
b. Installieren Sie EDR, AV und Velociraptor.
c. Erstelle neue DCs im green VLAN mit der neuesten OS-Version, installieren Sie alle Security Systeme und alle Rollen auf die neuen DCs migrieren.

4.1.6 Passwörter

a. Sobald der Domänencontroller wieder funktioniert, setzen Sie alle Konten zurück und erzwingen Sie sichere Passwörter mit einem Passwortgenerator.
b. Setzen Sie Ihr Kerberos Golden Ticket zweimal zurück (Neustart).
c. Alle Passwörter zurücksetzen, nicht nur Benutzer-AD-bezogene (Appliances,
Service Accounts, lokale Konten, ...).

4.1.7 Email

a. Sicherstellung, dass keine Mails verloren gehen. Erweitern Sie Ihre Anti-Spam-Lösung: Unzustellbarkeitszeit/Meldung (72h) und Dimensionierung.
b. Erwägen Sie eine vollständige Migration in die Cloud (O365).
c. Erstellen Sie Ihre E-Mail-Umgebung on-prem neu, falls bevorzugt.

4.1.8 Application Server

a. Wiederherstellung vom Backup im red VLAN mit AV, EDR und Velociraptor.
Neue Application Server mit AV und EDR im green VLAN erstellen.
b. Wiederherstellung von Daten (Greenwashing).
c. Besondere Überlegungen zu Legacy-Server
Wenn notwenig, komplett isoliert vom restlichen Netzwerk.

4.1.9 Daten Restore

a) Datenbanken, Benutzerdaten, Fileserver, ...
b) Daten Greenwashing (red -> orange -> green).

2 x Scan durch AV (evtl. Unterschiedliche AV)
Große Datenmenge in Paketen (wenn möglich)
Zeitfaktor ...

Wenn nicht möglich, alle Daten zu "waschen" isolieren Sie diese Daten.

4.1.10 Backup Planung

a. Neuer Backup Plan (Cloud / Drittanbieter) für alle Server im green VLAN.
b. Beginnen Sie damit, sobald die Server in Betrieb genommen werden.

4.1.11 Endpoints

a. Alle Endpoints müssen neu installiert werden.
   Domain Joined / Local Admin
   EDR und AV
   Planen Sie die volle Kontrolle über alle Endgeräte
b. Alle Endpoints in einem eigenen VLAN.

4.1.12 Zusätzliche Sicherheitsmaßnahmen

a) Authentifizierungsrichtlinien
b) Patch-Management-System
c) Setzen Sie Ihr KRBTGT alle 180 Tage zurück
d) Sichern Sie Ihre App-Server mithilfe von GPO oder App-Blockern/Software- Einschränkungen
e) Verwenden des höheren SMB-Protokolls
f) HTTPS verwenden
g) Höhere TLS- Version verwenden
h) Usw.

5 Kommunikation und Organisation

Die Kommunikation mit Kunden und Geschäftspartnern ist für das Management von größter Bedeutung, um die Kontinuität des Geschäftsbetriebs zu gewährleisten.

Nehmen Sie Kontakt zu den Kunden auf, um ihr Geschäft und die Auswirkungen des Angriffs zu verstehen.

Schaffen Sie einen „Puffer" zwischen IT-Managern und der Geschäftsleitung.

6 Organisation

Für einen Vorfall und die Kommunikation kann folgende Organisation eingerichtet werden:

a. Team 1 > Forensik
   Wie /Wer/Was/Wo/Wann wurde kompromittiert

b. Team 2 > Infrastruktur
   Wiederherstellung der Infrastruktur inklusive Backup

c. Team 3 > Benutzerumgebung
   Vorbereitung der Benutzer auf die neue Einrichtung
   (Änderung der Kennwörter, Verteilung der neuen Kennwörter an die Benutzer an allen Standorten usw.)

d. Team 4 > Organisatorische Tätigkeiten und Kommunikation
   Meldung an Datenschutzbehörden, Polizei usw.
   Kommunikation mit der Geschäftsführung z.B. alle 6 Stunden