CYBERARK®

HACKERANGRIFF (ZU) LEICHT GEMACHT | ANGRIFFE NACH GÄNGIGEM MUSTER

EINFÜHRUNG: EINE GÄNGIGE ANGRIFFSMETHODE

- 2015 gingen in der Ukraine die Lichter aus. Nachdem zwei der drei regionalen Stromversorger Opfer eines Cyberangriffs geworden waren, saßen rund 225.000 Haushalte im Dunkeln.
- Durch zusätzliche Maßnahmen erschwerten die Hacker eine schnelle Wiederherstellung der Systeme. Da ihre IT- und OT-Systeme vollständig gekapert waren, mussten die Energieunternehmen den Schaden an ihren quer über die Region verteilten Umspannstationen manuell beheben. Damit ist es Hackern erstmals gelungen, ein ganzes Stromnetz über das Internet lahmzulegen und so für einen großflächigen, mehrstündigen Stromausfall zu sorgen.
- **Zugleich ist dieses Ereignis ein erschreckendes Beispiel dafür, welchen Schaden Cyberkriminelle anrichten können, die Zugriff auf das Netzwerk eines Unternehmens erlangen. Dabei bedienten sie sich eines gängigen Angriffsmusters, das Unternehmen mit geeigneten vorbeugenden Maßnahmen durchaus hätten verhindern können.**

GÄNGIGE SCHRITTE KOMPLEXER ANGRIFFE: ERFAHREN SIE…

- …wie Angreifer durch Phishing-E-Mails in Netzwerke eindringen

- …wie Angreifer Anmeldedaten von kompromittierten Systemen entwenden und sich durch IT-/OT-Umgebungen bewegen

- …wie Angreifer die Systeme von Unternehmen mittels Malware übernehmen, und mit kostspieligen Folgen schwer beschädigen

- … wie Sie durch proaktive Maßnahmen den Angreifern das Handwerk legen und sie daran hindern, ihre eigentlichen Ziele zu erreichen

SCHRITT 1: PHISHING - WIE E-MAILS ANGREIFERN DEN WEG EBNEN

- 1 | Opfer öffnet Phishing-Mail

- 2 | Malware infiziert Endgerät

- 3 | Angreifer erhalten über Malware Zugriff auf Systeme

- 4 | Nutz- und Anmelde-daten werden entwendet

- **Erfolgschancen von Angreifern mindern:**
- Mitarbeiter sensibilisieren: E-Mails/Anhänge/ Links
- Regelmäßig Patches/ Updates aufspielen
- Kontrolle von Anwendungen und Anwendungsrechten auf Endgeräten
- Benutzern lokale Admin-Rechte generell entziehen

SCHRITT 2: DIEBSTAHL VON ANMELDEDATEN - WIE ANGREIFER IN IT- & OT-UMGEBUNGEN EINDRINGEN

- Angreifer stehlen lokale Admin-Passwörter

- Passwörter werden für Domain-Zugriff und Zugriffe auf weitere Systeme missbraucht

- Angreifer erlangen durch Rechteausweitung Kontrolle über IT-Netzwerk

- Kompromittierte (VPN)-Anmeldedaten ermöglichen Sprung ins OT-Netzwerk oder andere sensible Bereiche

- **Risikominderung eines Diebstahls von Anmeldedaten:**
- Mehrstufige Authentifizierung.
- Administrator-Passwörter regelmäßig ändern.
- Auf jedem System ein anderes lokales Administrator-Passwort.
- Sicherung privilegierter Accounts, wie Domänenkonten/ Konten mit Zugriff auf kritische Infrastruktur.
- Prüfung des Verhaltens privilegierter Benutzer/ Accounts auf ungewöhnliche Aktivitäten.
- Segmentierung sensibler Netzwerkbereiche und Isolierung privilegierter Zugriffe auf kritische Systeme.

DAS ZIEL: WIE ANGREIFER IHR BUSINESS LAHMLEGEN UND EINE WIEDERHERSTELLUNG VERHINDERN

- Angreifer schalten die Leitzentrale ab und damit den Betrieb von IT-Steuer-systemen und die Strom-versorgung

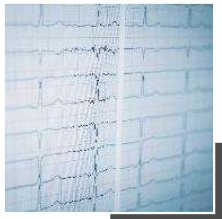
- Bösartige Firmware-Updates trennen Verbindun-gen und schädigen Hardware nachhaltig

- Daten auf IT-Systemen werden durch Malware über-schrieben

- DDoS-Angriff legt Leitungen zu Support lahm

- **Angreifer entdecken und Schäden minimieren:**
- Segmentierung von Netzwerken.
- Isolierung des Zugriffs auf kritische Systeme und Überwachen des eingehenden Datenverkehrs.
- Schutz und regelmäßige Änderung privilegierter Anmeldedaten
- Kontrolle und Überwachung von Anwendungen
- Prüfung des Verhaltens von Benutzern/ Accounts auf ungewöhnliche Aktivitäten – inkl. 4-Augen-Prinzip während der Tätigkeit.

FAZIT: 12 BEST PRACTICES ZUR VEREITELUNG GÄNGIGER ANGRIFFE



Schutz von Endgeräten

- 1 | Nutzer dazu anhalten, gegenüber unerwarteten E-Mails misstrauisch zu sein.
- 2 | Systeme regelmäßig patchen, um bekannte Schwachstellen zu eliminieren.
- 3 | Anwendungen und Anwendungsrechte kontrollieren, um das Risiko von Infektionen mit Malware zu senken.
- 4 | Standardbenutzern lokale Admin-Rechte entziehen.

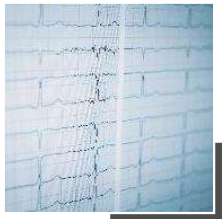
Sicherung & Kontrolle von Anmeldedaten

- 5 | So oft wie möglich eine mehrstufige Authentifizierung verwenden.
- 6 | Administrator-Passwörter regelmäßig ändern.
- 7 | (Lokale) Administrator-Passwörter nicht mehrfach verwenden.
- 8 | Privilegierte Accounts sichern und deren Nutzung überwachen.
- 9 | Netzwerke segmentieren, um den Zugriff auf sensible IT-Systeme einzuschränken.
- 10 | Zugriff auf kritische Systeme isolieren und einschränken.

Erkennung von Bedrohungen

- 11 | Verhalten von Benutzern und Accounts auf ungewöhnliche Aktivitäten prüfen.
- 12 | Aktivitäten in privilegierten Sessions überwachen, um Insider-Bedrohungen erkennen zu können.

WIE EIN „PAS HYGIENE PROGRAMM“ HELFEN KANN …



Schutz von Endgeräten

- 1 | Nutzer dazu anhalten, gegenüber unerwarteten E-Mails misstrauisch zu sein.
- 2 | Systeme regelmäßig patchen, um bekannte Schwachstellen zu eliminieren.
- **3 | Anwendungen kontrollieren, um das Risiko von Infektionen mit Malware zu senken.**
- **4 | Standardbenutzern lokale Admin-Rechte entziehen.**

Schutz & Kontrolle von Anmeldedaten

- **5 | So oft wie möglich eine mehrstufige Authentifizierung verwenden.**
- **6 | Administrator-Passwörter regelmäßig ändern.**
- **7 | Lokale Administrator-Passwörter nicht mehrfach verwenden.**
- **8 | Privilegierte Accounts schützen und deren Nutzung überwachen.**
- 9 | Netzwerke segmentieren, um den Zugriff auf sensible IT-Systeme einzuschränken.
- **10 | Zugriff auf kritische Systeme isolieren und einschränken.**

Erkennung von Bedrohungen

- **11 | Verhalten von Benutzern und Accounts auf ungewöhnliche Aktivitäten prüfen.**
- **12 | Aktivitäten in privilegierten Sessions überwachen, um Insider-Bedrohungen erkennen zu können.**

CYBERARK®

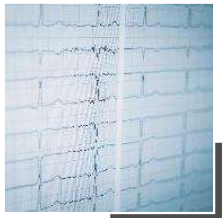
CYBERARK PAS HYGIENE PROGRAMM

VON EINFACHEN „HYGIENE-MAßNAHMEN“ BIS ZUR FORTGESCHRITTENEN SECURITY-STRATEGIE – PROAKTIVE ANSÄTZE, DIE AUF ERFAHRUNGSWERTEN BEKANNTGEWORDENER SICHERHEITSVORFÄLLE BASIEREN

ZIELE DES „PAS HYGIENE PROGRAMM“

- **Schritt 1:** Konzentration auf die Eliminierung irreversibler Netzwerkübernahmeangriffe (z. B. Golden Tickets in Kerberos)
- **Schritt 2:** Bekannte Infrastruktur-Accounts kontrollieren und sichern
- **Schritt 3:** Laterale Bewegung einschränken
- **Schritt 4:** Privilegierte Konten von Dritten schützen
- **Schritt 5:** SSH-Keys auf kritischen Unix-Servern verwalten
- **Schritt 6:** Cloud- und DevOps-Accounts verteidigen
- **Schritt 7:** Gemeinsam genutzte IDs von Geschäftsanwendern sichern (Umsetzung von MFA integrieren und beschleunigen)

WIE EIN „PAS HYGIENE PROGRAM“ VERHINDERN KANN…



Schutz von Endgeräten

- 1 | Nutzer dazu anhalten, gegenüber unerwarteten E-Mails misstrauisch zu sein.
- 2 | Systeme regelmäßig patchen, um bekannte Schwachstellen zu eliminieren.
- **3 | Anwendungen kontrollieren, um das Risiko von Infektionen mit Malware zu senken.**
- **4 | Standardbenutzern lokale Admin-Rechte entziehen.**

Schutz & Kontrolle von Anmeldedaten

- **5 | So oft wie möglich eine mehrstufige Authentifizierung verwenden.**
- **6 | Administrator-Passwörter regelmäßig ändern.**
- **7 | (Lokale) Administrator-Passwörter nicht mehrfach verwenden.**
- **8 | Privilegierte Accounts schützen und deren Nutzung überwachen.**
- 9 | Netzwerke segmentieren, um den Zugriff auf sensible IT-Systeme einzuschränken.
- **10 | Zugriff auf kritische Systeme isolieren und einschränken.**

Erkennung von Bedrohungen

- **11 | Verhalten von Benutzern und Accounts auf ungewöhnliche Aktivitäten prüfen.**
- **12 | Aktivitäten in privilegierten Sessions überwachen, um Insider-Bedrohungen erkennen zu können.**

CYBERARK®

PRIVILEGED ACCOUNT SECURITY
=
PRIVILEGED IDENTITY PROTECT PRO

HTTPS://CLOUD.TELEKOM.DE/MAGENTA-SECURITY/PRIVILEGED-IDENTITY-PROTECT-PRO/