END CYBER RISK

JEDE MINUTE ZÄHLT

DIE ARCTIC WOLF INCIDENT RESPONSE TIMELINE

JEDE MINUTE ZÄHLT

Die Arctic Wolf Incident Response Timeline

Wenn Hacker in IT-Systeme eindringen, ist zeitnahes Handeln wichtig. Ganz klar: Je länger die Angreifer ihr Unwesen treiben können, desto größer ist der Schaden.

Quelle: https://www.ibm.com/security/data-breach

END CYBER RISK

Der Faktor Zeit entscheidet über das Ausmaß des Schadens und den damit verbundenen Kosten. Dabei ist sich die Fachwelt uneinig, wie lange es durchschnittlich dauert bis Unternehmen Cyberangriffe entdecken. Sind es 11 Tage oder sogar deutlich mehr?

Die Wahrheit ist: Der Unterschied ist im Grunde unerheblich.

Denn bereits alles, was länger als eine Stunde dauert, erhöht den Schaden für die betroffenen Unternehmen erheblich. Laut einer **Studie des Ponemon Institute** belaufen sich die durchschnittlichen Kosten auf 7,12 Millionen US-Dollar, wenn Cyberangriffe in weniger als 30 Tagen entdeckt werden. Braucht ein Unternehmen mehr als 90 Tage, verdoppelt sich der Schaden.

Um die Auswirkungen eines Cyberangriffs deutlich zu begrenzen, geht es heute nicht mehr um Tage – jede Minute zählt.

Unternehmen müssen demnach nicht nur alles tun, um Cyberangriffe abzuwehren. Im Fall des Falles geht es vor allem darum, einen aus Sicht der Hacker erfolgreichen Angriff möglichst schnell zu entdecken und sofort Gegenmaßnahmen einzuleiten – ein Wettlauf mit der Zeit.

Eine gängige Möglichkeit, Cyberattacken zu erkennen, sind Security-Information & Event-Management-Systeme (SIEM), die Sicherheitsvorfälle in Echtzeit analysieren und Alarme auslösen. Das SIEM-System erkennt zum Beispiel Trends und Muster, die vom üblichen Schema abweichen und auf einen Angriff hindeuten.

ALARMFLUT SENKT **AUFMERKSAMKEIT**

Ein häufig auftretendes Problem von SIEM-Plattformen ist jedoch: Sie erzeugen eine Menge „Rauschen“ in Form von Fehlalarmen.

Aus Risikosicht ist das zunächst durchaus nachvollziehbar: Besser ein Alarm zu viel als einer zu wenig. Andererseits führt ein Übermaß an Fehlalarmen zu einer sogenannten „Alert Fatigue“, einer gewissen Trägheit und Überforderung der IT-Security-Abteilungen, die bereits mit ihren alltäglichen Aufgaben mehr als ausgelastet sind.

Gleichzeitig nehmen Umfang und Schwere der Bedrohungen zu und der Markt für qualifizierte Cybersecurity-Fachkräfte ist äußerst begrenzt.

Darüber hinaus können SIEM-Lösungen ein falsches Gefühl von Sicherheit vermitteln. Sie sammeln und analysieren große Datenmengen, oftmals jedoch nicht von allen IT-Systemen. So entstehen potenziell gefährliche blinde Flecken.

Es ist also keine Überraschung, wenn Unternehmen Schwierigkeiten haben, auf die ständig steigenden Cyber-Bedrohungen schnell und effektiv zu reagieren.

DIE VERLÄNGERTE CYBERSECURITY-WERKBANK
TRIAGE- UND CONCIERGE-SECURITY-TEAMS

Arctic Wolf bietet Services, die Unternehmen dabei unterstützen, Angriffe schnell zu erkennen und zu beheben.

Dazu kombiniert Arctic Wolf die eigene Plattform-Technologie mit menschlicher Expertise in Form von **Triage- und Concierge-Security-Teams (CST)**.

Das Triage-Team konzentriert sich darauf, wie bei einem Security-Vorfall taktisch vorzugehen ist. Erkennt die Arctic Wolf Plattform eine Anomalie, leitet das Triage-Team eine Untersuchung ein, um die Bedrohung zu bestätigen oder zu widerlegen. Anschließend teilt ein fest dem Kunden zugeordneter Sicherheitsexperte die Ergebnisse der Untersuchung mit.

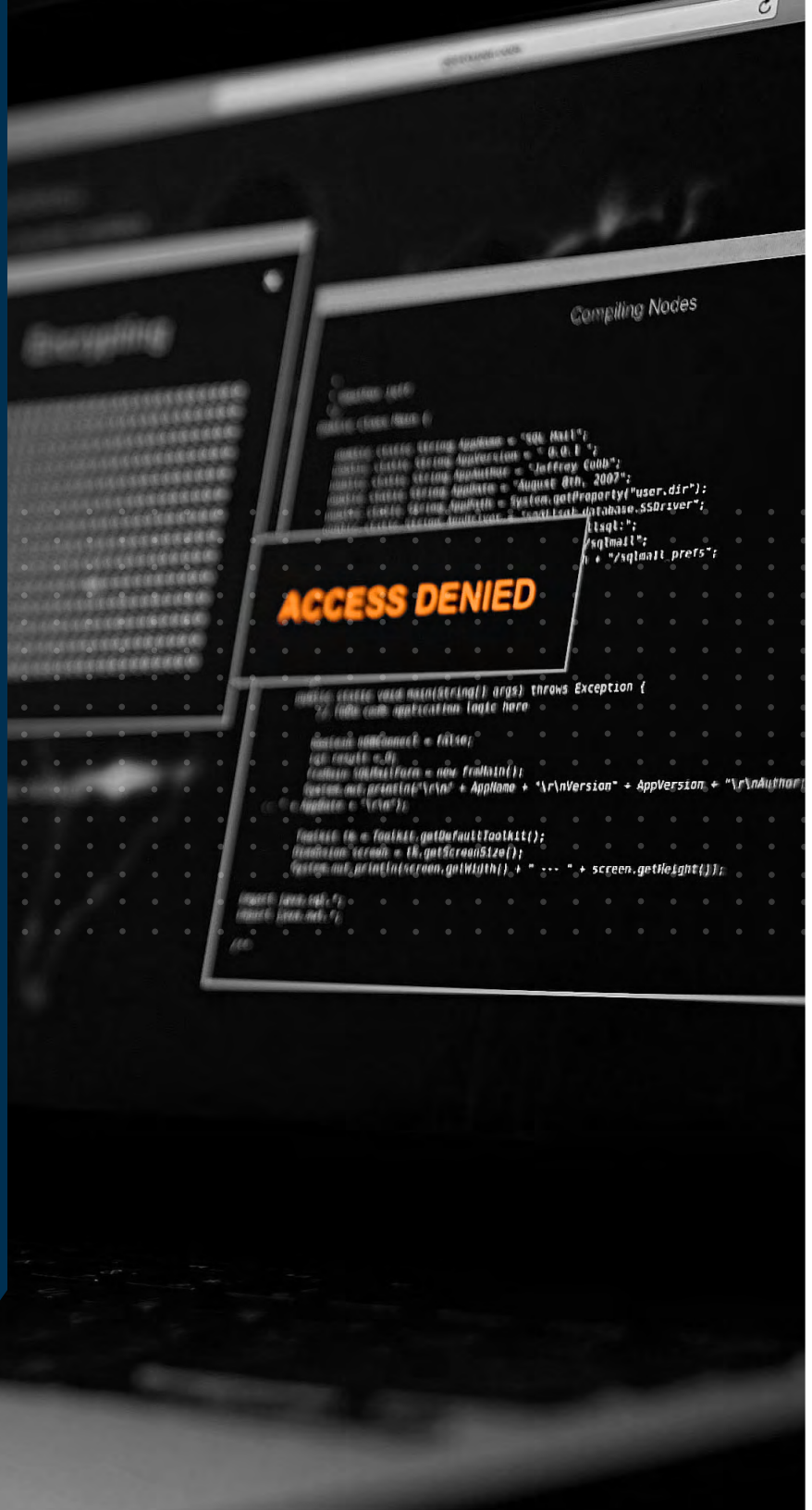
Dies kann von einer einfachen Benachrichtigung bis hin zu einer engen Zusammenarbeit mit dem Kunden reichen, bis der Vorfall gelöst ist.

Das Concierge-Security-Team konzentriert sich auf die Kundenbeziehung und die strategischen Auswirkungen eines Angriffs. Immer mit dem Ziel, Sicherheitsabläufe langfristig zu verbessern.

Das Team unterstützt Kunden dabei, Verbesserungsmöglichkeiten zu erkennen und Schwachstellen zu beseitigen. Dafür nutzt das Concierge-Security-Team die detaillierten Analysen des Vorfalls des Triage-Teams.

Zeit ist entscheidend

Wie die Zusammenarbeit zwischen dem Triage- und Concierge-Security-Team von Arctic Wolf und Unternehmen konkret aussieht, zeigen reale Sicherheitsvorfälle, die in der Vergangenheit von den Teams bearbeitet wurden.



RANSOMWARE ANGRIFF AUF EINE KOMMUNALVERWALTUNG

Angriffstyp
Ransomware Angriff

Zeit bis Erkennung
5:23 – 5:28 Uhr | 5 Minuten

Quellen
Active Directory
Arctic Wolf Sensor

Arctic Wolf-Plattform | Arctic Wolf Triage-Team | Kunde | CST

5:23 Uhr

Quelle: Active Directory

- Ein Benutzerkonto beginnt sich bei mehreren Systemen anzumelden.

5:26 Uhr

Quelle: Arctic Wolf Sensor

- HTTP-Header-Informationen mit ausgehender Kommunikation mit xx.xxx.230.236 entdeckt, möglicherweise C2.
- Verdächtige PowerShell Empire-Aktivität auf einem Server entdeckt.

5:28 Uhr

Investigation wird angestoßen

- Investigation wird angestoßen. C2-Verkehr korreliert mit PowerShell Empire-Aktivität auf dem Server.
- Der Vorfall wird zum Triage-Team Level 3 via einem forensischen Dashboards mit Dringlichkeitsstatus eskaliert.

5:29 Uhr

Investigation beginnt

- Das Triage-Team beginnt mit der Untersuchung und findet Aktivitäten in den Active Directory Logs des Benutzers, der sich in kürzester Zeit bei vielen Systemen angemeldet hat.
- Das Triage-Team bestätigt und bewertet einen Angriff.

5:48 Uhr

Investigation abgeschlossen

Das Triage-Team kontaktiert den Kunden mit einer Dokumentation mit detaillierten Angaben zum C2-Verkehr sowie den Anmeldungen, die diesen Verbindungen vorausgingen. Es wird eine Empfehlung ausgesprochen:

- Sperren Sie das Gerät, trennen Sie die Verbindung zum Netzwerk.
- Ändern Sie Passwörter für Konten des betroffenen Anwenders.
- Tätigen Sie einen AV-Scan auf den Endpunkten.

6:13 Uhr

Wiederherstellung

- Der Kunde bestätigt, dass das Gerät gesperrt und die Passwörter zurückgesetzt wurden.

Security Journey

Anschließend entwickelt das CST mit dem Kunden eine Verbesserung der Sicherheitslage und empfiehlt folgende Maßnahmen:

- Umsetzung des Prinzips der geringsten Privilegien für Remote Tools
- **Geofence Firewalls – Firewall-Funktion, die die geografische Region identifiziert, aus der der Datenverkehr stammt**
- **MFA-Aktivierung (Multifaktor-Authentifizierung)**
- **Group Policy Object (GPO): Gruppenrichtlinienobjekt einrichten, um die Verwendung von PowerShell zu blockieren**
- **Installation von Arctic Wolf Agent mit Sysmon auf allen Rechnern**

Sysmon (SystemMonitor) ist ein Windows-Systemdienst- und Gerätetreiber, der die Systemaktivität im Windows Ereignisprotokoll überwacht und protokolliert.

E-MAIL-KOMPROMITTIERUNG BEI EINEM FERTIGUNGSUNTERNEHMEN

Angriffstyp
Übernahme des E-Mail-Accounts

Zeit bis Erkennung
12:57 - 13:16 Uhr | 19 Minuten

Quellen
Office 365
Duo

Arctic Wolf-Plattform | Arctic Wolf Triage-Team | Kunde | CST | Angreifer

12:57 Uhr

- Angreifer nutzt gestohlene Anmeldeinformationen und sendet Duo-MFA-Push-Benachrichtigungen an legitimen Anwender.
- Dieser akzeptiert die Duo-MFA-Push-Benachrichtigung.
- Angreifer stellt ActiveSync mit der Mailbox des Benutzers her.

13:16 Uhr

- Angreifer öffnet bestehenden Kalendereintrag und aktualisiert ihn mit eigenen Informationen.
- Angreifer fügt Weiterleitungs- und Löschregeln zur Inbox.

13:18 Uhr

- Triage-Team beginnt Untersuchung.

13:25 Uhr

- Triage-Team benachrichtigt den Kunden, dass ein Benutzer kompromittiert wurde.
- Es empfiehlt die Deaktivierung des Accounts und Zurücksetzen der Anmeldedaten.

13:31 Uhr

- CST kontrolliert zusammen mit dem Kunden die Log-Daten aller Nutzerkonten, die auf Phishing-PDF zugreifen können.
- Das Concierge-Security-Team bestätigt, dass keine Anwender auf die PDF-Datei zugegriffen haben.

Quelle: Duo

- Arctic-Wolf-Plattform protokolliert MFA.

12:57 Uhr

Source: Office 365 Logs

- Die Plattform eskaliert den Vorfall, nachdem erkannt wird, dass im Benutzerkonto Regeln hinzugefügt und gelöscht werden.

13:17 Uhr

- Angreifer lädt Phishing-PDFs auf OneDrive, um diese per E-Mail an die Teilnehmenden der Kalendereinträgen zu versenden.

13:22 Uhr

- Kunde bestätigt die Kompromittierung und deaktiviert das Konto.

13:25 Uhr

EXCHANGE EXPLOIT BEI BAUUNTERNEHMEN

Angriffstyp
Ausnutzung einer Schwachstelle

Zeit bis Erkennung
19:27 - 19:29 Uhr | 2 Minuten

Quellen
Arctic Wolf Agent
Arctic Wolf Sensor
SentinelOne

Arctic Wolf-Plattform | Arctic Wolf Triage-Team | Kunde | CST | Anhaltendes Monitoring durch Arctic Wolf

Montag, 2. August

- Kunde vervollständigt 30-tägiges Onboarding und Servicebereitstellung beginnt.

Samstag, 7. August 19:27 Uhr

Quelle: Arctic Wolf Agent

- Arctic Wolf Agent erkennt eine PowerShell-Enumeration von Befehlen auf Exchange.

19:29 - 19:47 Uhr

- Das Triage-Team bestätigt, dass die Enumeration-Befehle verdächtig sind und es möglicherweise ein Ryuk ist.
- Das Team erstellt ein Ticket und kontaktiert den Kunden.

Ryuk ist eine Ransomware-Variante der Hackergruppe WIZARD SPIDER, die bereits Regierungen, Bildungseinrichtungen, Gesundheitsdienstleister, Fertigungsunternehmen und Technologieanbieter angegriffen hat.

19:50 Uhr

Quelle: Arctic Wolf Agent

- SVN.exe auf Exchange abgelegt.
- PowerShell-Befehl “svn.exe-verbinden 135.181.x.x:443 -Pass Pasword123”.

Quelle: Arctic Wolf Sensor

*** IP 135.181.x.x ist verbunden mit C2-Server in Finnland.**

20:08 Uhr

Quelle: Arctic Wolf Agent

- **User1 zu Exchange in lokaler Administratoren-Gruppe hinzugefügt.**
- **Anmeldeinformationen für lokales Admin-Konto wurden zurückgesetzt.**

20:09 Uhr

Quelle: SentinelOne / Arctic Wolf Agent

- Versuchte laterale Bewegung mit Nutzerkonto zu 2 Geräten.
- Kunde setzt Exchange-Server offline und ist mit dieser Maßnahme vorerst zufrieden.

Eine laterale Bewegung ist der Prozess, durch den sich Cyberkriminelle von einem Eintrittspunkt aus auf den Rest des Netzwerks ausbreiten.

Wiederherstellung

- Das CST entwickelt mit dem Kunden Schritt für Schritt in einer Zoom-Konferenz Maßnahmen, um bestehendes Problem zu lösen.
- Es werden SVN.exe und Benutzerkonto gelöscht und das Admin-Konto zurückgesetzt.
- Die Anmeldeinformationen für alle zwischengespeicherten Anwender auf Exchange werden zurückgesetzt.
- Es werden alle Domänen-Anmeldeinformationen zurückgesetzt, die nach dem 7. August auf den Server zugegriffen haben.
- Externe Verbindungen zum Exchange-Server werden geschlossen.

Montag, 9. August

Security Journey

- Danach erfolgt zusätzlich eine Sicherheitsprüfung durch das CST.
- Es wird ein Schwachstellen-Scan auf Exchange durchgeführt, durch den festgestellt wird, dass kritische Exchange-Patches nicht realisiert wurden, die mehr als 6 Monate zurückliegen, einschließlich Zero-Days.
- Der Kunde bestätigt, dass sein 3rd-Party-Patching-Tool nicht richtig funktioniert.
- Das CST liefert ein Skript zur Identifizierung von Exchange-Verletzungen vor dem Onboarding von Arctic Wolf.
- Das Skript findet eine Backdoor: ASP/Buonpower.A!dha.
- Das vorhandene Webshell wird entfernt. MFA für VPN und Office 365 aktiviert und ein GPO zur Verhinderung einer Enumeration erstellt.

PASSWORD SPRAYING BEI EINER KANZLEI

Angriffstyp
Password Spray

Zeit bis Erkennung
18:24 - 18:45 Uhr | 21 Minuten

Quellen
On-Premise
Active Directory

Arctic Wolf-Plattform | Arctic Wolf Triage-Team | Kunde | CST

18:24 Uhr

- Arctic-Wolf-Plattform ermittelt durch einen Zugang zum On-Premises Active Directory des Kunden die erste Reihe von fehlgeschlagenen Windows-Anmeldungen.

18:45 Uhr

- Arctic-Wolf-Plattform erkennt das Ende der Windows-Anmeldefehler.

19:03 Uhr

- Arctic Wolf Rules Engine führt eine Analyse durch und identifiziert 20 Anmeldeversuche innerhalb von 5 Minuten von 10 verschiedenen Benutzernamen mit derselben IP-Adresse.

19:03 Uhr

- Das Triage Team erhält Informationen über den Vorfall.

19:08 Uhr

- Fünf Minuten später erstellt ein Analyst des Triage-Teams ein Ticket für den Vorfall – 102 fehlgeschlagene Anmeldungen mit 10 verschiedenen Benutzernamen von einem einzigen internen System.

19:12 Uhr

- Der Kunde erhält eine Benachrichtigung und einen Report, der detailliert aufführt, dass es sich um einen Penetrationstest handelt – was der Kunde bestätigt.

9:00 Uhr

- Am nächsten Tag bespricht das CST den Vorfall mit dem Kunden, um Möglichkeiten zur Verbesserung der Sicherheitsumgebung des Kunden zu ermitteln.

DER SCHLÜSSEL ZU **EFFEKTIVEN SICHERHEITSMASSNAHMEN**

Der Unterschied zwischen einem fehlgeschlagenen und einem erfolgreichen Angriff hängt oft von der Geschwindigkeit des Vorgehens ab. Je schneller Angreifer Schwachstellen erkennen und ausnutzen können, desto wahrscheinlicher ist es, dass sie ihre Ziele erreichen. Umgekehrt gilt: Je länger ein Unternehmen benötigt, um zu reagieren, desto größer ist die Wahrscheinlichkeit, dass es Opfer eines Angriffs wird.

Unternehmen nutzen strategische Sicherheitspartner, die Bedrohungen schnell erkennen und deren Ursachen analysieren können. Diese Partner müssen darüber hinaus in der Lage sein, die Bedrohungsanalyse mit fundiertem Know-how über die gesamte Sicherheitsumgebung auszuführen und konkrete Maßnahmen zur Verbesserung der Sicherheitslage des Unternehmens umzusetzen. Dazu benötigen sie einen Überblick über die gesamte Angriffslage, um Bedrohungen zu erkennen und die Ereignisse effektiv zu korrelieren.

Die Arctic-Wolf-Plattform sowie das Triage- und Concierge-Security-Team von Arctic Wolf bieten einen umfassenden skalierbaren Ansatz für Security Operations.Arctic Wolf agiert schnell und effektiv.

Jede Umgebung ist einzigartig und hat ihre eigenen Anforderungen an die Cybersicherheit.

Erfahren Sie, was Arctic Wolf für Ihr Unternehmen tun kann.

Vereinbaren Sie Ihre Demo.

END CYBER RISK

ÜBER ARCTIC WOLF

Arctic Wolf® ist ein weltweiter Marktführer im Bereich Security Operations und bietet die erste cloudnative Security-Operations-Plattform zur Abwehr von Cyber-Risiken. Basierend auf ThreatTelemetry, die Endpunkt-, Netzwerk- und Cloud-Quellen umfasst, analysiert die Arctic Wolf® Security Operations Cloud weltweit mehr als 1,9 Billionen Security Events pro Woche. Sie liefert unternehmenskritische Erkenntnisse zu nahezu allen Security Use Cases und optimiert die heterogenen Sicherheitslösungen der Kunden. Die Arctic Wolf® Plattform ist bei mehr als 2.700 Kunden weltweit im Einsatz. Sie bietet automatisierte Threat Detection und Response und ermöglicht es Unternehmen jeder Größe, auf Knopfdruck erstklassige Security Operations einzurichten.

Weitere Informationen über Arctic Wolf finden Sie unter **www.arcticwolf.com** oder Sie folgen uns auf **Twitter**, **LinkedIn** oder **Facebook**.

DEMO VEREINBAREN

ARCTIC WOLF

SOC2 TYPE II CERTIFIED

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

KONTAKT

arcticwolf.com
ask@arcticwolf.com