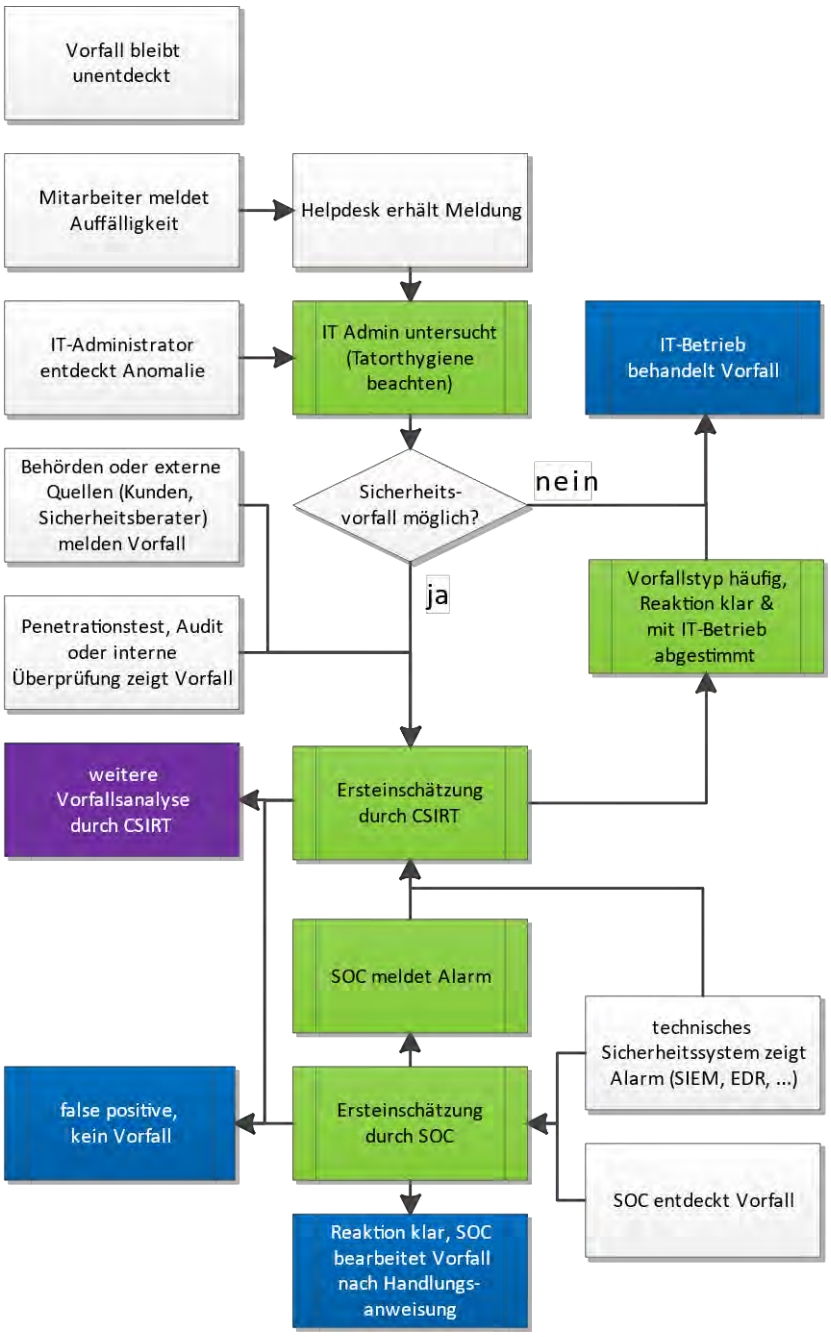
Alarmstufen im ISMS

Viele Unternehmen haben einen CISO bestellt, einen Verantwortlichen für die Informationssicherheit, der meist als neutrales Kontrollorgan neben dem IT-Leiter agiert und direkt an das Management berichtet. Die Aufgabe des IT-Leiters ist es, die IT als Dienstleister für das eigene Business zu positionieren und die Digitalisierung im Unternehmen voranzutreiben. Die wesentliche Aufgabe des CISO wiederum ist es, die Informationen und Systeme des Unternehmens vor absichtlichen Angriffen und versehentlichem Datenabfluss zu schützen. Durch die Rollentrennung werden Diskussionen ausgelöst und so bessere Kompromisse gefunden. Die meisten CISOs bauen für die Arbeit ihrer Organisationseinheit ein Information Security Management System (ISMS) auf. Dies ist vornehmlich auch die Grundlage für Zertifizierungen, z. B. nach ISO 27001. Häufig wird in einem ISMS der Fokus auf die präventive Sicherheitsarbeit gelegt: Sicherheits-Policies und Vorgaben sowie deren Kontrollen stehen im Fokus des kontinuierlichen Verbesserungsprozesses.

Reaktive Sicherheit als Aufgabe der CISO-Organisation

In einer Zeit steigender Angriffszahlen kann sich kein CISO allein auf die präventive Arbeit beschränken. Tritt ein Vorfall ein, wird die Geschäftsführung als Erstes auf den Verantwortlichen für die IT-Sicherheit im Unternehmen schauen. In klassischen Krisen treten Symptome fast immer offensichtlich zutage und Fehlerquellen sind größtenteils mit einem geschulten Auge schnell ersichtlich und einfach erklärbar. Symptome von Angriffen und potenzielle Fehlerquellen in IT-Systemen sind auch für Experten nicht auf den ersten Blick erkenntlich. Es liegt daher im Eigeninteresse des CISO, dass Alarme in einem geregelten Prozess frühzeitig erkannt und behandelt werden. *Das Cyber-Security-Krisenmanagement benötigt Prozesse für die Suche nach Vorfällen!* Die Entdeckung und richtige Klassifizierung eines Vorfalls spielen in der reaktiven IT-Sicherheit eine außerordentlich wichtige Rolle. Ein Grund dafür ist, dass bei einem Cyber-Sicherheitsvorfall (hauptsächlich in den frühen Stadien, z. B. beim „initial compromise“ oder dem „lateral movement“) keine offensichtlichen Symptome vorhanden sein müssen. Als Konsequenz gilt der Grundsatz, dass effektives Cyber-Security-Krisenmanagement schon vor Eintritt eines Cyber-Sicherheitsvorfalls mit der Suche nach Symptomen beginnt.



Die wichtigste reaktive Aufgabe der CISO-Organisation ist es, dafür zu sorgen, dass ein Cyber-Sicherheitsvorfall überhaupt entdeckt wird. Wichtige Maßnahmen sind:

- Etablieren der Sicherheitsstrategien “Assume Breach” und “Defense in Depth”
- Sensibilisierung der (IT-)Mitarbeiter
- Regelmäßige Auswertung der Sicherheitsprotokolle von wichtigen IT-Systemen/-Komponenten
- Awareness-Schulungen für Führungskräfte und Mitarbeiter
- Durchführung regelmäßiger interner und externer Audits, Penetrationstests, Red-Team-Tests und Vulnerability Scans auf verschiedene Bereiche, idealerweise in einem mehrjährigen Auditplan organisiert
- Aktive Suche im Internet nach Hinweisen auf Cyber-Sicherheitsvorfälle bei Ihrem Unternehmen (z. B. verdächtige Foreneinträge, Zugriff auf unternehmensinterne Dokumente mit Vertraulichkeitsklassifizierung „vertraulich“ oder „streng vertraulich“)

- Bei besonders hohem Risiko: Regelmäßige IT-forensische Untersuchung von besonders exponierten und zusätzlich einigen zufällig ausgewählten IT-Systemen nach unbekannter Schadsoftware

Die Suche darf dabei nicht auf die IT beschränkt sein: Produktionssysteme (Operational Technology, OT) und Entwicklungssysteme (Engineering Technology, ET) müssen einbezogen werden. Auch externe Hinweise (z. B. Angebotssummen werden vorab bekannt) müssen als sicherheitsrelevantes Ereignis erkannt und gemeldet werden. Die Ereignisse müssen in der CISO-Organisation bewertet und miteinander verknüpft werden. Dazu müssen verschiedene Melde- und Eingangswege überwacht werden:

- Unternehmenseigene Sicherheitsstellen, IT bzw. Helpdesk erhalten Meldung von internen Mitarbeitern oder externen Entitäten (z. B. Kunden)
- Hinweise durch aktive Suche von IT oder CISO-Abteilung (siehe oben)
- IT-Administratoren entdecken Anomalie
- Hinweise aus technischen Systemen (SIEM)
- Hinweis kommt vom externen Security Operation Center
- Hinweis kommt von Behörden oder externen Quellen

Auf dieser Basis muss dann eine einheitliche Behandlung eines Vorfalls sichergestellt werden, egal wo ein Vorfall oder Verdacht detektiert oder gemeldet wurde. Es darf keine doppelten Taskforces oder parallel arbeitende Gremien geben. Das Motto ist: *viele Meldewege, einheitliche Behandlung.*

Je besser die Meldewege funktionieren, je mehr „Assume Breach" in einem Unternehmen gemacht wird, je mehr auch das interne Netz überwacht wird, desto häufiger kommen Alarmmeldungen. Damit ergibt sich ein neues Problem: Was ist zu tun, wenn die Meldesysteme mit Warnungen anschlagen, ohne gleich einen roten Alarm zu melden? Kann man das einfach weglächeln? Wenn nicht, was muss nun passieren? Während in einem „echten" Ransomwarefall der Schaden bereits eingetreten ist, gibt es nun zwei mögliche Ergebnisvarianten:

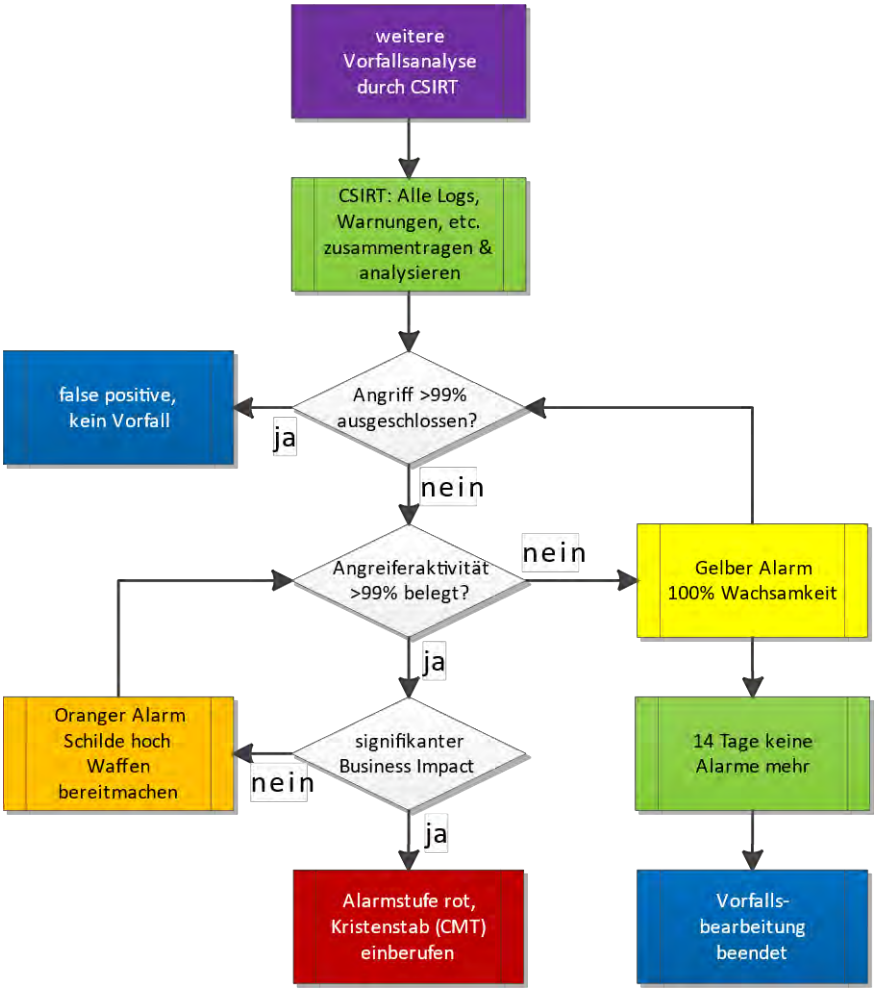
- Entweder die Warnungen waren „false positives" oder – häufiger – nicht von einem Angreifer, sondern einer Fehlfunktion oder einer Fehlbedienung verursacht, oder
- Es ist ein Angreifer im Netzwerk, dessen Präsenz die Umsetzung von Maßnahmen außerhalb des normalen täglichen Prozessablaufs erfordert.

Die CISO-Organisation muss dafür Sorge tragen, dass unternehmensintern die Abläufe zur Behandlung von Cyber-Sicherheitsvorfällen etabliert und bekannt sind. Zu einer minimalen Vorbereitung der Cyber-Sicherheitsvorfalls-Behandlung gehören beispielsweise:

- Definition von Alarmstufen
    - Welche Alarmstufen gibt es?
    - Was muss bei einer Ersteinschätzung beachtet werden?
    - Wie kann ein Verdacht konkretisiert werden?
    - Bei welchen Ereignissen wird welche Alarmstufe durch wen ausgelöst?
    - Welche Maßnahmen werden bei welcher Alarmstufe ausgelöst?
- Definierter Prozess zur Behandlung von Vorfällen
    - Wer ist wofür verantwortlich?
    - Wer hat in welchem Fall welche Aufgaben?
    - Wer berichtet an wen?
    - Wer darf welche Entscheidungen (z. B. die Ausrufung einer Alarmstufe) treffen?
    - Welche Hierarchieebenen dürfen in welchem Fall übersprungen werden?
    - Wer kontaktiert bei welchen Ereignissen externe Spezialisten (wie eine IT-Krisenhotline oder einen Forensiker)?
    - Wer koordiniert unternehmensintern die Maßnahmen?

Diese Festlegungen werden in einem Notfallhandbuch dokumentiert. In diesem stehen dann auch die wichtigsten Kontaktdaten (z. B. Krisenhotline und unternehmensinterne Entscheidungsträger). Ziel ist

es, dass das Unternehmen in der Lage ist, bei plötzlich auftretenden bedeutenden IT-Sicherheitsvorfällen selbstbestimmend und angemessen zu reagieren. Die CISO-Organisation benötigt dazu neben den präventiv arbeitenden Kräften einen reaktiv arbeitenden Organisationsteil. Diese Einheit in der normalen Aufbauorganisation wird meist CSIRT oder CERT genannt, unterscheidet sich aber signifikant von dem im Krisenfall benötigten IT-Notfallstab, der oft genauso genannt wird. Ein Prozess dazu könnt z. B. so aussehen:



Vorbereitungen für das Alarmstufenmanagement

Die CISO-Organisation muss für den Alarmfall die notwendigen rechtlichen Regelungen in Zusammenarbeit z. B. mit der Mitarbeitervertretung (Betriebsrat) und dem Datenschutz unternehmensintern im Vorfeld vereinbaren:

- Regelung des Umfangs der Privatnutzung von Systemen, E-Mail und Internet, sodass im Notfall eine forensische Auswertung möglich ist
- Regelung der Auswertung von Daten bei Cyber-Sicherheitsvorfällen oder dem Verdacht auf schwere Pflichtverletzungen/strafbare Handlungen
- Regelung der Auswertung von System-Backups zur Aufklärung von Cyber-Sicherheitsvorfällen
- Regelung der Entscheidungsbefugnisse, Zustimmungs- und Informationspflichten, auch bei Vorfällen außerhalb der regulären Betriebszeiten
- Regelung der Bereitstellung relevanter Daten durch den IT-Dienstleister bzw. Cloud-Anbieter
- Prüfung der Relevanz weiterer gesetzlicher Regelungen im IT-Betrieb (z. B. Fernmeldegeheimnis § 88 TKG)

Ziel ist es, dass die rechtlichen Rahmenbedingungen eine erfolgreiche und schnelle Ermittlungsarbeit bei Verdacht auf einen Cyber-Sicherheitsvorfall ermöglicht.

Die Erfahrung zeigt, dass neben dem Krisenfall (Alarmstufe rot) auch Maßnahmen zumindest die Alarmstufen orange und gelb definiert werden müssen. Ebenso müssen Kriterien für die Rückkehr zum normalen Arbeitsmodus („grün“) festgelegt werden. Eine frühzeitige Definition der Alarmstufen hilft der IT, auch in Sondersituationen einen klaren Kopf zu bewahren. Die Kommunikation dieser Stufen ans Management erleichtert im Ernstfall den Transport komplexer Risiken, ohne die Führungsebene zu verschrecken und hilft, Aktionismus zu minimieren. Allerdings müssen dazu sowohl die eigene Organisation als auch die Organisationen der Cloud-Anbieter und Dienstleister organisatorisch in der Lage sein, eine Alarmstufen-Situation auch kompetent mit Leben zu füllen. Die gute Nachricht ist: Übungen können entfallen – solide präventive IT-Sicherheitssysteme vorausgesetzt, kommt die nächste Übungssituation innerhalb von 6 Monaten automatisch.

Die wichtigsten Vorbereitungen für die beiden Alarmstufen „gelb“ und „orange“ ist die Definition eines Management Sponsors und seines Stellvertreters. Empfehlenswert ist es, dass über die Alarmstufe Gelb der IT-Leiter, über Orange ein Vorstand bzw. Geschäftsführer entscheidet. Der jeweilige Manager liefert ein klar definiertes Management Commitment und stellt ein kleines Team aus IT-Spezialisten zusammen. Fallweise werden auch Experten aus den Fachbereichen bzw. der Produktion benötigt. Typischerweise werden 1–3 IT-Know-how Träger in Vollzeit (freigestellt von allen anderen Aufgaben) und ein Sicherheitsspezialist, der weiß, wie Angreifer heute vorgehen, benötigt. Idealerweise ist das Know-how rund um Netzwerk, Firewall, WAN, AD und Endpoint Security / Malware / Virenschutz vertreten. Der Manager ist im Verlauf der Arbeit auch die Stelle, an die sich das Team wendet, um den Business Impact von Maßnahmen oder um sich Kommunikation an die Mitarbeiterschaft abzustimmen und freigeben zu lassen. Ein täglicher Statusbericht vom Team an den Sponsor hat sich bewährt.

Typische weitere Vorbereitungen sind eine Schutzbedarfsanalyse in Bezug auf Verfügbarkeit („Business Impact Analyse“ mit „Recovery Time Objective“ und „Recovery Point Objective“), inklusive eventueller Gefahren in der physischen Welt durch Steuergeräte, OT oder Ähnliches. Ein gutes Verständnis der Hotline und Helpdesk Prozesse ist hilfreich, um Meldungen der Mitarbeiterschaft zu kanalisieren. Oft wird auch ein temporäres, intensives 24/7 Monitoring gebraucht. Im Vorfeld zu klären, wie man eine solche Überwachung beauftragen kann, hilft im Echtfall. Oft übernehmen Cyberversicherungen auch bestimmte Deckungen im Verdachtsfall. Es lohnt sich, den internen Verantwortlichen für die Cyberversicherung darauf anzusprechen.

Tatorthygiene für Administratoren

Oft werden Anomalien von IT-Administratoren zuerst entdeckt und untersucht. Im Polizeijargon: die IT-Admins sind regelmäßig die Ersten am Tatort. Jeder Administrator im Unternehmen sollte daher die Grundlagen für die Erstanalyse eines Vorfalls kennen. So kann sichergestellt werden, dass zu Beginn einer Untersuchung (etwa einer Anomalie auf einem Server) keine eventuell später relevanten Informationen vernichtet werden. Ziel einer Erstuntersuchung ist unter anderem die Einstufung einer entdeckten Anomalie in die Kategorien „sicherheitsrelevant“ oder „nicht sicherheitsrelevant“. Diese Einstufung muss jeder Administrator aus seiner eigenen Erfahrung beurteilen.

Die Erstreaktion basiert auf dem Prinzip

Protokollieren – Konservieren – Analysieren – Melden

Protokollieren (1): Alle eigenen Tätigkeiten während der Untersuchung einer Anomalie *nachvollziehbar* protokollieren. Wer? Wie? Wann? Wo? Warum? Ein kurzer Stichpunktzettel reicht.

Protokollieren (2): Alle gewonnenen Erkenntnisse während der Untersuchung (Fakten und Interpretationen) protokollieren. Wer? Wie? Wann? Wo? Warum? Ein kurzer Stichpunktzettel reicht.

Insbesondere beim „Wann?“ sind die entsprechend relevanten Zeitstempel wichtig. Nicht nur der Zeitpunkt der Untersuchung, sondern auch die Datumswerte von Logeinträgen oder Dateien werden beim späteren Aufbau einer Timeline eine wichtige Rolle spielen.

Konservieren (1): Wenn möglich, den aktuellen Systemzustand frühzeitig vor dessen Veränderung (!) für eine spätere Analyse konservieren. Dies kann z. B. durch einen Snapshot (bei virtuellen Maschinen bzw. SAN-Speicher), ein Backup (Idealumfang: gesamte Installation; minimal: alle Logdateien) oder den Ausbau der Festplatte und Einbau einer neuen Festplatte vor einer Neuinstallation geschehen.

Konservieren (2): Wenn sich der Verdacht auf einen Sicherheitsvorfall erhärtet, sollten alle aktiven Verfahren zur Datenlöschung (Logrotation, Expiration von Backups und SAN-Snapshots etc.) außer Kraft gesetzt werden – zumindest lokal, im Idealfall auf allen Kernsystemen (Firewalls, Logarchiv, Backup-System, Monitoring-Stationen etc.).

Analysieren: So wenig „Trial-and-Error“ wie möglich! Das Credo der Untersuchung sollte sein: „Zunächst nur analysieren, später umkonfigurieren!“ Im Idealfall werden keine Veränderungen am System vorgenommen, bevor die Problemursache nicht zweifelsfrei ermittelt und dokumentiert ist oder eine vollständige und konsistente Sicherungskopie der betroffenen Systeme erstellt wurde. Anmerkung: Der vorsorgliche Neustart eines Systems ist eine Veränderung.

Melden: Management frühzeitig involvieren, melden macht frei. Wenn sich der Verdacht auf einen Sicherheitsvorfall erhärtet, keine(!) weiteren Veränderungen an Systemen und/oder Applikationen durchführen, sondern so schnell wie möglich die zuständigen Abteilungen (Sicherheitsverantwortlicher, CISO) oder das Management (IT-Leiter, Geschäftsführung) verständigen. Dabei die im Unternehmen bestehenden Meldewege beachten, um den geordneten Start der vordefinierten Prozesse sicherzustellen.

Wenn die Meldung dann bei den entsprechenden Sicherheitsverantwortlichen eingeht, muss eine abgestufte Reaktion erfolgen.

Alarmstufe Gelb: 100% Wachsamkeit

Alarmstufe gelb wird ausgerufen, wenn die Warnungen folgender Definition genügen: *Nachdem alle derzeit bekannten Fakten (Logeinträge, Warnungen, etc.) zusammengetragen wurden, kann nicht sicher ausgeschlossen werden, dass es sich um einen Echtangriff nach einem bereits bekannten Muster handelt.* Es könnte zwar sein, dass es sich nur um eine normale Betriebsstörung handelt. Es mag sogar wahrscheinlich so sein, aber eine wirkliche Erklärung existiert noch nicht.

Grundsätzlich gilt, dass in einem „gelb“ Fall mit den Maßnahmen nicht mehr Schaden angerichtet werden darf als unbedingt notwendig. Es dürfen also für „gelb“ nur Vorgaben gemacht werden, die in einer durchschnittlichen IT-Infrastruktur mit durchschnittlichen IT-Admins kaum Business Impact entfalten. Ziel der Maßnahmen muss sein, entweder einen Angriff ausschließen zu können oder einen belegbaren Hinweis für eine maliziöse oder zumindest unberechtigte Aktivität eines Angreifers zu finden. Das Ziel dieser Stufe ist die Aufklärung eines noch vagen Verdachts. Die Hauptaufgabe ist dementsprechend die *Schaffung einer angemessenen Sichtbarkeit innerhalb der IT-Systeme*. Typische Werkzeuge dazu sind:

- Überprüfung oder Implementierung der Advanced Audit Policy
- Erweiterung der Firewall-Protokolle auf vollständige Sichtbarkeit in Bezug auf die gesamte Kommunikation mit den anderen Netzwerkteilen.
- Aktivieren des Reputationsdienst Ihrer ausgehenden Firewall (um C2-Verbindungen zu finden).
- Stoppen der Protokollrotation und sichern der Protokolle aller relevanten Systeme (AD, Firewall, Virenscanner, Sysmon (Ereignisprotokolle))

- Etablierung einer schnellen Recherche- und Auswertungsmöglichkeit (SIEM, Splunk, Graylog, etc.). Alternative Excel- oder UNIX-Befehlszeilentools, ggf. mit externer Unterstützung (Manpower).
- In Zeiten, in denen kein aktives Sicherheitsmonitoring stattfindet, die "Full Auto Remediation" in der der-Lösung zu aktivieren.
- Überwachung typischer Alarmbedingungen:
    - Neuanlage von Admin-Benutzern
    - Änderungen an Gruppenrichtlinienobjekten
    - Änderungen an geplanten Aufgaben / Scheduled Tasks
    - Änderungen im Sysvol
    - Ausführung von PSExec oder Angreifertools (z. B. Mimikatz, Cobaltstrike, Bloodhound)
    - Erhöhte WMI-Aktivitäten oder massenhafte LDAP-Abfragen gegen das AD

Eine der wichtigsten Maßnahmen ist es allerdings ab Alarmstufe gelb das wichtigste Sicherheitsnetz Ihres Unternehmens zu überwachen: Ihr Backupsystem.

- Ist das Backup außerhalb der Reichweite eines Remote-Angreifers aufbewahrt („offline")? Befinden sich die wichtigsten Systeme des Backups in einem eigenen Segment? Sind die administrativen Zugänge gesichert (Jump-Host, MFA, keine Domänenkonten zur Administration)?
- Werden alle Systeme gesichert (Vollständigkeit)?
- Stimmt der Umfang der Sicherung?
- Funktioniert die Wiederherstellung? Wann war der letzte Test?

Selbstverständlich enthält der Werkzeugkasten der Alarmstufe gelb aber auch aktive Maßnahmen:

- Sicherstellen, dass das Patch-Management auf dem neuesten Stand ist. Insbesondere die Patch-Level der Tier-0-Systeme (Domaincontroller, Backupsysteme, Verwaltungsrechner der virtuellen Maschinen, Firewallmanagement, etc.) und alle am Vorfall beteiligten Systeme ist zu prüfen.
- Scannen der auffälligen und der kritischen Systeme mit einem Scanner wie dem MS Safety Scanner[1]
- Schaffung der Transparenz bzgl. der Angreifbarkeit der eigenen Domäne durch einen Ping-Castle-Scan[2] mit anschließender Überwachung der Schwachpunkte
- Überprüfen der Firewall-Regeln
- Alle Benutzer in Verbindung mit dem Vorfall sollten ihr Kennwort zurücksetzen
- OPTIONAL: Verwenden eines sicheren DNS-Servers (z. B. Quad9)

Im Rahmen des täglichen Statusberichts an den Management-Sponsor muss das Team darstellen, wie weit die Detaillierung der auslösenden Warnung fortgeschritten ist. Zudem wird eine Einschätzung benötigt, ob und wie schnell weitere Angreiferaktivitäten entdeckt werden würden. Sollten die ursprünglichen Warnungen weder in die eine noch in die andere Richtung aufgeklärt werden können, so sollte die erhöhte Wachsamkeit der Alarmstufe gelb nach zwei Wochen ohne weitere Vorkommnisse beendet werden. In diesem Fall ist aber ein Lesson Learned Workshop notwendig, um die Konfiguration der Systeme so zu ändern, dass beim nächsten Vorfall eine definitive Aussage möglich wird. Falls noch nicht geschehen, sollte die Umsetzung der Corporate Trust Mindeststandards aus Kapitel nun starten.

Alarmstufe Orange: Schilde hoch, Waffen bereit machen

Alarmstufe orange tritt in Kraft, wenn folgende Situation eintritt: *In den derzeit bekannten Fakten befinden sich belegbare Hinweise für eine maliziöse oder zumindest unberechtigte Aktivität eines Angreifers. Es ist bis jetzt noch kein echter Schaden in den Kernprozessen des Unternehmens*

[1] https://docs.microsoft.com/de-de/windows/security/threat-protection/intelligence/safety-scanner-download)
[2] https://pingcastle.com/

entstanden, ein Angriff ist aber im Gang. Vergleichbar ist die Situation mit einer Kameraüberwachung, die ein neu geschnittenes Loch im Zaun des Unternehmens aufzeigt. Die jetzt zu treffenden Sicherheitsmaßnahmen dürfen Business Impact haben. Sie müssen sie aber geeignet sein, das klare Ziel, einen – jetzt sicher zu erwartenden – Schaden vom Unternehmen abzuhalten, zu erreichen.

Die Alarmstufe orange wurde ausgelöst, da eine Angreiferaktivität sicher detektiert wurde. *Zusätzlich zum Monitoring aus der Alarmstufe gelb* sind inzwischen zwei weitere Handlungsfelder zu bearbeiten. Zum einen müssen die Angreifer aus dem Netzwerk entfernt, zum anderen der Ernstfall vorbereitet werden. Die typischen Aktionen zur Entfernung der Täter aus dem Netzwerk sind im Einzelfall sehr unterschiedlich. Um einen Eindruck von den möglichen Maßnahmen zu vermitteln, haben wir einige häufiger benutzte Vorgehensweisen ausgewählt:

- Verwenden eines sicheren DNS-Server (z. B. Quad9)
- Aufbau eines Web-Proxies mit einer Internet-Whitelist. Alternativ können am Webfilter der Firewall die generischen Kategorien abgeschaltet werden. Einschalten eines Filters für ausgehende Ports an der Firewall. Dies behindert zwar die Surf-Aktivitäten der Mitarbeiter, die Remote Access Fähigkeit der Angreifer werden aber ebenso gestört.
- Durchführung von forensischen Analysen von befallenen Rechnern und Reverse Engineering aufgefundener Schadsoftware. Ziel ist dabei nicht die Befriedigung technischer Neugier, sondern die Identifikation sogenannter „Indicators of Compromise“ (IoCs). Diese IP-Adressen, URLs oder File Hashes können dann in der ganzen IT gesucht werden, um weitere befallene Systeme zu identifizieren.
- Sofortiges Patchen aller Systeme, die nicht auf dem aktuellen Patchstand sind, insbesondere aller Tier0 Rechner und aller von extern erreichbaren Computer. Altsysteme, die noch in der Domäne und ohne Segmentierung betrieben werden, müssen nun temporär abgeschaltet werden.
- Falls noch nicht bereitgestellt: Einführung eines EDR-Systems so schnell wie möglich (z. B. Defender for Endpoint). Aktivieren des Modus "automatische Behebung".
- Installieren vom MS Defender for Identity auf dem Domänencontroller (und Ihrem EDR-System oder zumindest Sysmon).
- Aufbau zweier neuer, aktueller DCs mit einer neuen Installationsdatei von Microsoft („Clean Source“). Aktivierung aller aktuellen Sicherheits-Features auf diesen DCs. Nachdem die neuen DCs in Sync sind, alle bisherigen DCs demoten und einstweilen stilllegen.
- Wenn der Verdacht besteht, dass die Angreifer bereits über Passwörter der Mitarbeiter verfügen: Sofortiges Aktivieren der MFA für alle externen Zugänge zum Unternehmensnetzwerk, Abschalten von Remote-Einwahlen, wo dies nicht möglich ist, zurücksetzen aller von außen ohne MFA nutzbaren Passwörter (z. B. zu Clouddiensten, Office365, etc.).
- Ändern aller Admin- und Dienstkonto-Passwörter. Falls noch nicht geschehen, Umbenennen von Standardbenutzern (z. B. "Administrator") und Erstellung personalisierter Administratorkonten.
- Sollte eine 24/7 Überwachungsmöglichkeit nicht vorhanden sein, sind Sofortmaßnahmen zur Netztrennung einzuleiten. Insbesondere eine sofortige Trennung der Produktion von der IT oder eine Trennung des Internet über Nacht und am Wochenende ergibt Sinn.

Die Vorbereitungshandlungen für den Ernstfall sind idealerweise bereits im Krisenhandbuch beschrieben. Wichtige Maßnahmen sind:

- Kommunikation des Status Alarmstufe „orange“ an die Mitarbeiter, idealerweise in einer Form, dass kein Alarm an die Tagespresse dringt. Ein vorgefertigter Kommunikationsblock für die Führungsebene und eine Hotline für Fragen und zur Meldung verdächtiger Aktivitäten für die Mitarbeiter leisten meist gute Dienste.

- Neben der Absicherung des Backups (siehe oben) kann die Schaffung von „Cold-Standby“ Systemen durch Klonen kritischer IT-Strukturen in der virtuellen Umgebung später einen Zeitvorsprung bei der Wiederherstellung schaffen

Die Alarmstufe orange hat einen Sponsor aus dem Top-Management. Diesem wird im Rahmen des täglichen Statusberichts dargestellt, wie weit die Angreiferaktivitäten aufgeklärt sind. Der Sponsor koordiniert auch die Vorbereitungshandlungen für die Einberufung des unternehmensweiten Krisenstabs für den Fall einer Eskalation der Lage.

Autor: Florian Oelmaier

Prokurist, Leiter IT-Sicherheit & Computerkriminalität, IT-Krisenmanagement
https://twitter.com/h0tz3npl0tz

CORPORATE TRUST
Business Risk & Crisis Management GmbH
Graf-zu-Castell-Straße 1
D-81829 München

Tel.: +49 89 599 88 75 80
info@corporate-trust.de
www.corporate-trust.de
blog.corporate-trust.de