37. Jahrgang / Nr. 6, Dezember 2021
ISSN 1611-440X
HZ208190

<kes>

Die Zeitschrift für Informations-Sicherheit

BSI Forum
offizielles Organ des BSI

Bundesamt
für Sicherheit in der
Informationstechnik

DevSecOps:
Kultur für Security by Design

S. 25

Alarmzustand:
Sicherheit braucht mehr als „rot“ und „grün“

S. 12

Aufgabenflut für CISO & Co.
– eindämmen und abgrenzen

S. 6

DATAKONTEXT

DEFCON 2 – Alarmstufe Orange?

Notfall- und Alarm-Zustände für die Informations-Sicherheit

Die Welt ist voller Grautöne – und auch in Sachen Informations-Sicherheit genügen die beiden Zustände „alles auf Grün" und „roter Alarm" heute nicht mehr. Unser Autor beschreibt daher sinnvolle Zwischentöne zur Alarmierung beziehungsweise Mobilisierung von Kräften der Security-Abteilung und Mechanismen des Business-Continuity-Managements (BCM).

Von Florian Oelmaier, München

Beim Business-Continuity-Management (BCM) für die IT hat sich viel getan – und nicht ohne Grund: Nahezu täglich liest man neue Meldungen über Unternehmen, bei denen sich die Folgen von Cybersecurity-Bedrohungen auf die Lieferfähigkeiten auswirken. Übungen für Ransomware-Krisen gehören mittlerweile zum „guten Ton" im BCM (vgl. etwa [1]). Auch angepasste Krisenpläne und -handbücher sind in vielen Unternehmen verfügbar, in denen Notfallmaßnahmen – beispielsweise im Fall einer Ransomware-Attacke – klar geregelt sind: Server werden abgeschaltet, Internetverbindungen getrennt und die Security-Truppen zusammengerufen. Aber auch präventive technische Schutzmaßnahmen wie Endpoint-Detection und -Response (EDR / XDR) oder von einem Security-Operations-Center (SOC) betriebene Security-Information- (oder sogar: -Incident-) und -Event-Managementsysteme (SIEM) sind mittlerweile mehr oder minder flächendeckend im Einsatz (vgl. [2]).

Jedoch wissen auch die Angreifer um neue technische Möglichkeiten der Verteidiger und versuchen, zunehmend unauffälliger vorzugehen. Damit ergibt sich immer häufiger ein neues Problem: Was kann man tun, wenn die Meldesysteme mit Warnungen anschlagen, ohne gleich einen roten Alarm zu melden? Kann man das einfach weglächeln? Wenn nicht: Welche Teile der BCM-Prozesse müssen dann schon anlaufen? Während in einem „echten" BCM-Fall der Schaden bereits eingetreten ist, gibt es hier zwei mögliche Ergebnisvarianten:

_____ Entweder die Warnungen waren „False Positives" oder – häufiger – nicht durch einen Angreifer, sondern eine Fehlfunktion oder eine Fehlbedienung verursacht, oder

_____ es befindet sich ein Angreifer im Netzwerk, dessen Präsenz die Umsetzung von Maßnahmen außerhalb des normalen täglichen Prozessablaufs erfordert, um die Business-Continuity zu gewährleisten.

Aus diesen Überlegungen heraus ergibt sich eine zusätzliche Aufgabe des BCM: Neben dem Krisenfall (Alarmstufe Rot) müssen auch Maßnahmen für weitere Alarmstufen Orange und Gelb definiert werden – überdies benötigt man Kriterien für die Rückkehr zum normalen Arbeitsmodus (Status Grün).

Definitionen

_____ **Alarmstufe Gelb:** Nachdem man alle zurzeit bekannten Fakten (Logeinträge, Warnungen etc.) zusammengetragen hat, kann nicht ausgeschlossen werden, dass es sich um einen tatsächlichen Angriff nach einem bereits bekannten Muster handelt. Die bekannten Muster sollten dem eigenen Security-Team, einem beauftragten Sicherheitsberater oder SOC-Dienstleister bekannt sein – ansonsten hilft ein Studium der MITRE Tactics, Techniques and Procedures (TTP) auf https://attack.mitre.org/. Grundsätzlich gilt, dass man in einem „Gelb-Fall" mit den ergriffenen Maßnahmen nicht mehr Schaden anrichten darf als unbedingt erforderlich. Daher dürfen für „gelb" nur Vorgaben gemacht werden, die in einer durchschnittlichen IT-Infrastruktur mit durchschnittlichen IT-Admins kaum Business-Impact entfalten! Ziel der Maßnahmen muss es sein, entweder einen Angriff ausschließen zu können oder einen belegbaren Hinweis für eine böswillige oder zumindest unberechtigte Aktivität eines Angreifers zu finden.

_____ **Alarmstufe Orange:** Die zurzeit bekannten Fakten umfassen belegbare Hinweise für eine böswillige oder zumindest unberechtigte Aktivität eines Angreifers. Es ist zwar noch kein echter Schaden in den Kernprozessen des Unternehmens entstanden, wohl aber ein Angriff im Gang. Vergleichbar ist diese Situation mit einer Kameraüberwachung, die ein frisch geschnittenes Loch im Zaun des Unternehmens aufzeigt. Die nun zu treffenden Sicherheitsmaßnahmen dürfen zwar Business-Impact haben, müssen aber klar dazu geeignet sein, einen – jetzt sicher zu erwartenden – Schaden vom Unternehmen fernzuhalten.

Vorbereitung

Die wichtigsten Vorbereitungen für die beiden Alarmstufen ist die Definition eines *Management-Sponsors* und seines Stellvertreters. Empfehlenswert ist, dass über die Alarmstufe Gelb der IT-Leiter, über Orange ein Vorstand oder Geschäftsführer entscheidet. Der jeweilige Manager liefert dabei ein klar definiertes Management-Commitment und stellt ein kleines Team aus IT-Spezialisten zusammen. Typischerweise benötigt man hierzu ein bis drei IT-Know-how-Träger in Vollzeit (freigestellt von allen anderen Aufgaben) und einen Sicherheitsspezialisten, der weiß, wie Angreifer heute vorgehen. Idealerweise ist auch Know-how rund um Netzwerk, Firewall, WAN, AD und Endpoint-Security / Malware / Virenschutz vertreten. Der Manager ist im Verlauf der Arbeit gleichzeitig auch die Stelle, an die sich das Team wendet, um den Business-Impact von Maßnahmen oder die 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,* inklusive eventueller Gefahren in der physischen Welt durch Steuergeräte, Operational Technology (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 – schon im Vorfeld zu klären, wie man eine solche Überwachung beauftragen kann, hilft im Echtfall.

Gelber Alarm: 100 % Wachsamkeit

Das Ziel dieser Stufe ist die *Aufklärung* eines noch vagen Verdachts – die Hauptaufgabe ist dementsprechend, eine angemessene Sichtbarkeit innerhalb der IT-Systeme zu schaffen. Typische Werkzeuge dazu sind:

_____ Stopp der Log-Rotation und Sichern relevanter Logs quer über die Systeme (AD, Firewall, Virenscanner, Sysmon)

_____ Aufbau einer schnellen Recherche- und Auswerte-Möglichkeit der relevanten Logs: Wo bereits ein SIEM oder Log-Analyse-Tool (z. B. Splunk, Graylog, ELK etc.) vorhanden ist, kann das genutzt werden – ansonsten ist der mühsame Weg über Excel oder Unix-Commandline-Tools notwendig.

_____ Überwachung von typischen Alarm-Konditionen: zum Beispiel der Neuanlage von Admin-Benutzern, Änderungen in den Gruppenrichtlinien (Group Policy Objects – GPO), den Scheduled Tasks oder im Sysvol, die Ausführung des Remote-Tools PSExec oder anderer „Hackertools" (wie Mimikatz, Cobaltstrike oder Bloodhound) oder auch erhöhte WMI-Aktivitäten.

_____ Schaffung von Transparenz bezüglich der Angreifbarkeit der eigenen Domäne: etwa durch einen Pingcastle-Scan mit anschließender Überwachung der Schwachpunkte

Selbstverständlich enthält der Werkzeugkasten der Alarmstufe Gelb aber auch aktive Maßnahmen: Ein Scan auffälliger Systeme mit dem Microsoft Safety Scanner (https://docs.microsoft.com/de-de/windows/security/threat-protection/intelligence/safety-scanner-download), die Einführung einer Advanced Audit-Policy in der Domäne und das „Hochdrehen" von Firewall-Logs sind typische Werkzeuge dieser Stufe. Oft wird auch der Domain-Name-Service (DNS) auf einen sicheren DNS-Server umgeschwenkt (z. B. Quad 9), der Reputation-Service der Firewall aktiviert oder verschärft, um Command-and-Control-(C&C)-Traffic zu blocken. In Zeiten, in denen kein aktives Sicherheitsmonitoring stattfindet, hilft es außerdem, Funktionen zur „Full Auto Remediation" in der eingesetzten EDR-Lösung zu aktivieren.

Eine besonders wichtige Maßnahme ist zudem ab jetzt das wichtigste Sicherheitsnetz des eigenen Unternehmens zu überwachen: das Backup-System. Werden alle Systeme gesichert? Stimmt der Umfang der Sicherung? Befindet sich das Backup außerhalb der Reichweite eines Remote-Angreifers („offline")?

Im Rahmen des täglichen Statusberichts an den Management-Sponsor muss das Team darstellen, wie weit die Detaillierung der auslösenden Warnung fortgeschritten ist. Zudem benötigt man eine Einschätzung, ob und wie schnell sich weitere Angreifer-Aktivitäten entdecken ließen. Sollten die ursprünglichen Warnungen weder in die eine noch in die andere Richtung aufgeklärt werden können, dann sollte die erhöhte Wachsamkeit der Alarmstufe Gelb nach zwei Wochen ohne weitere Vorkommnisse enden. In diesem Fall ist aber ein „Lessons-Learned"-Workshop notwendig, um die Konfiguration der Systeme so zu ändern, dass beim nächsten Vorfall eine definitive Aussage möglich wird.

Oranger Alarm: Schilde hoch, Waffen bereitmachen!

Die Alarmstufe Orange kommt zum Einsatz, wenn eine offensive Aktivität sicher detektiert wurde. Zusätzlich zum Monitoring aus der Alarmstufe Gelb sind nun zwei weitere Handlungsfelder zu bearbeiten: Zum einen müs-

sen die Angreifer aus dem Netzwerk entfernt, zum anderen der Ernstfall vorbereitet werden.

Aktionen zur Entfernung von Angreifern sind im Einzelfall sehr unterschiedlich. Die folgende Auflistung ausgewählter, häufiger benutzter Vorgehensweisen sollte jedoch einen guten Eindruck von den möglichen Maßnahmen vermitteln:

_____ Aufbau eines Web-Proxies mit einer Internet-Whitelist – alternativ können am Webfilter der Firewall die generischen Kategorien abgeschaltet werden – sowie Einschalten eines Filters für ausgehende Ports an der Firewall: Dies behindert zwar auch Surf-Aktivitäten der Mitarbeiter, die Remote-Access-Fähigkeit von Angreifern wird aber ebenso gestört.

_____ Durchführung forensischer Analysen von befallenen Rechnern und Reverse-Engineering aufgefundener Schadsoftware: Ziel ist dabei nicht die Befriedigung technischer Neugier, sondern die Identifikation von Indicators of Compromise (IoCs) – hieraus resultierende IP-Adressen, URLs oder File-Hashes können dann in der gesamten IT gesucht werden, um weitere befallene Systeme zu identifizieren.

_____ Sofortiges Patchen aller Systeme, die nicht auf dem aktuellen Patchstand sind, insbesondere aller von extern erreichbaren Computer – Altsysteme, die noch in der Domäne und ohne Segmentierung betrieben werden, sind temporär abzuschalten

_____ Aufbau zweier neuer, aktueller Domain-Controller (DCs) mit einer „frischen" Installationsdatei von Microsoft (Clean Source!) sowie Aktivierung aller aktuellen Sicherheits-Features auf diesen DCs: Nachdem die neuen DCs „in sync" sind, muss man alle bisherigen DCs „demoten" und vorübergehend stilllegen.

_____ Wenn der Verdacht besteht, dass Angreifer bereits über Passwörter der Mitarbeiter verfügen: sofortiges Aktivieren einer Multi-Faktor-Authentifizierung (MFA) für alle externen Zugänge zum Unternehmensnetzwerk, Abschalten von Remote-Einwahlen, Reset aller von außen nutzbaren Passwörter.

_____ Sollte eine 24/7 Überwachungsmöglichkeit nicht vorhanden sein, sind Sofortmaßnahmen zur Netztrennung einzuleiten: zum Beispiel eine sofortige Separation der Produktion von der IT oder eine Trennung des Internet über Nacht und am Wochenende

Alle erforderlichen und vorhersehbaren *Vorbereitungshandlungen für den Ernstfall* sollten idealerweise bereits im Krisenhandbuch beschrieben sein – zwei wichtige derartige Maßnahmen sind beispielsweise:

_____ Kommunikation des Status „Alarmstufe Orange" an die Mitarbeiter – idealerweise in einer Form, dass keine Informationen an die Tagespresse dringen können: Ein vorgefertigter Kommunikationsblock für die Führungsebene und eine Hotline für Fragen sowie zur Meldung verdächtiger Aktivitäten für die Mitarbeiter leisten an dieser Stelle meist gute Dienste.

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

Fazit

Eine frühzeitige Definition verschiedener Alarmstufen hilft der IT, auch in Ausnahmesituationen einen klaren Kopf zu bewahren. Die Kommunikation dieser Stufen an das Management erleichtert im Ernstfall den Transport komplexer Risiken, ohne die Führungseben zu verschrecken, und hilft, Aktionismus zu minimieren.

Allerdings müssen dazu sowohl die eigene Organisation als auch genutzte Cloud-Anbieter und Dienstleister organisatorisch in der Lage sein, eine Alarmstufen-Situation kompetent mit Leben zu füllen! Die gute Nachricht ist: Übungen kann man dann ausfallen lassen – denn, solide präventive IT-Sicherheitssysteme vorausgesetzt, ergibt sich die nächste „Übungssituation" innerhalb von sechs Monaten ganz automatisch aus externen Aktivitäten beziehungsweise einem ausgerufenen Alarmzustand. ■

Literatur

[1] Falko Weiß, 12 Schnelltests für die Cyber-Security, <kes> 2021#4, S. 12

[2] Florian Oelmaier, Un-ver-zicht-bar!, 20 technische Mindeststandards zur Abwehr von Ransomware, <kes> 2020#6, S. 6

Florian Oelmaier ist Leiter IT-Sicherheit & Computerkriminalität, IT-Krisenmanagement bei der Corporate Trust, Business Risk & Crisis Management GmbH. Als @h0tz3npl0tz twittert er tagesaktuell wichtige Empfehlungen zur Cyber-Defense.