sure[secure]
your security operations center

secure mag

Don't Detect in the Dark - Preparation First

Technische Resilienz beginnt mit Sichtbarkeit und Struktur

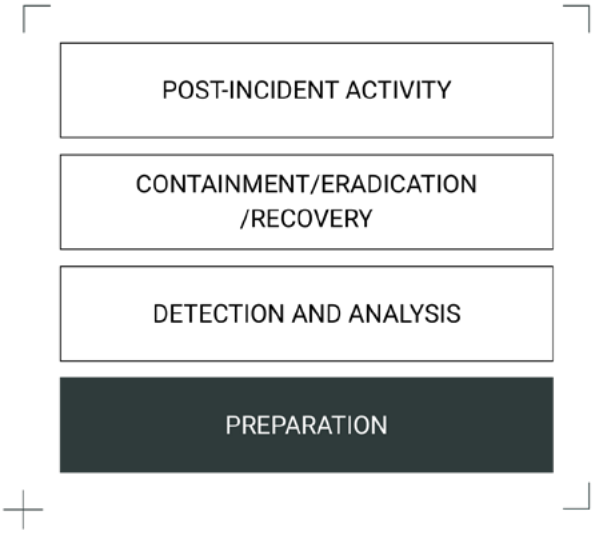
Es sind nicht die lautesten Angriffe, die Unternehmen in die Knie zwingen. Oft ist es das Unentdeckte, das Unerwartete, das Unvorbereitete. Während Firewalls flimmern und Endpoints geschützt werden, bleibt die eigentliche Schwachstelle bestehen: die mangelnde Vorbereitung. Die Frage ist nicht, ob ein Sicherheitsvorfall eintreten wird. Die Frage ist, wie gut wir darauf vorbereitet sind. Denn in der Stunde der Entscheidung entscheidet nicht die Technologie - sondern der Zustand der Organisation.

Wir widmen uns der oft unterschätzten ersten Phase des Incident Response Prozesses nach NIST 800-61: der Preparation. Wir beleuchten, warum diese Phase mehr ist als Dokumentation und Infrastrukturpflege. Preparation bedeutet strategische Weitsicht, technische Sorgfalt und organisatorische Disziplin. Sie ist der Faktor, der im Ernstfall über Minuten, Stunden und letztlich über Vertrauen und Zukunft entscheidet.

Andre Ditzel, Senior IR-Analyst, suresecure GmbH

Der Rahmen: NIST 800-61 und der Platz der Preparation

Das NIST Special Publication 800-61 stellt ein etabliertes Framework für Incident Response dar. Es unterteilt den Prozess in vier Phasen: Preparation, Detection and Analysis, Containment/Eradication/Recovery und Post-Incident Activity. Die Preparation ist dabei nicht nur der Ausgangspunkt, sondern das Fundament. Ihre Qualität bestimmt, wie effizient alle nachfolgenden Schritte ablaufen. Wer hier zu oberflächlich agiert, zahlt im Ernstfall mit Zeit, Unsicherheit und erhöhtem Schaden.



Preparation umfasst organisatorische, prozessuale und technische Maßnahmen. Sie definiert Rollen, schafft Sichtbarkeit, etabliert Kommunikationswege und hält Werkzeuge bereit, die im Fall eines Incidents zur schnellen Reaktion befähigen. Sie verlangt vorausschauendes Handeln und regelmäßige Selbstprüfung, nicht zuletzt, weil sich Bedrohungslagen und IT-Landschaften dynamisch verändern.

Organisatorische Readiness

Ein Incident Response Management Plan (IRMP) ist das Rückgrat jeder Preparation. Doch ein PDF im Intranet reicht nicht aus. Entscheidend ist, ob dieser Plan auch wirklich gelebt wird. Kennt jede betroffene Rolle ihre Aufgaben? Gibt es Stellvertretungsregelungen? Sind Kommunikationswege auch dann nutzbar, wenn Mailserver und VPN-Dienste versagen?

Ein funktionierender IRMP beschreibt nicht nur Verantwortlichkeiten, sondern verankert sie im Alltag. Er muss dynamisch sein, auf Änderungen in der Infrastruktur, Personalrotation oder neue regulatorische Anforderungen reagieren. Regelmäßige Reviews und Überprüfungen im Rahmen von internen Audits oder externen Simulationen sind essenziell. Denn ein IRMP ist kein statisches Dokument, sondern ein lebendiges Instrument zur Risikominderung.

Technische Preparation

Im Zentrum der technischen Vorbereitung steht die Frage: Können wir sehen, was passiert? Logs sind das Gedächtnis unserer Systeme. Doch was nützt ein Gedächtnis, das schweigt oder unvollständig ist? In lokalen Umgebungen stellt sich die Herausforderung, dass Systeme heterogen sind. Windows-Clients, Linux-Server, Netzwerkkomponenten, Firewalls - jedes System spricht seine eigene Sprache.

Für Trainings- und Analysezwecke kann es sinnvoll sein, aktuelle Sicherheitsvorfälle aus der Fachpresse oder von CERTs zum Anlass zu nehmen, um das eigene Logging und die vorhandene Sichtbarkeit zu hinterfragen. Häufig enthalten diese Berichte konkrete technische Details - etwa zur Angriffssequenz, zu verwendeten Tools oder zu relevanten Logeinträgen.

Diese Informationen lassen sich gemeinsam im Team durchgehen und mit der eigenen Infrastruktur abgleichen: Welche der genannten Events wären in der aktuellen Umgebung überhaupt erfassbar? Existieren dafür geeignete Logquellen? Werden diese gespeichert, korreliert und ausgewertet?

Solche Diskussionen können nicht nur Awareness schaffen, sondern auch zur konkreten Ableitung technischer Maßnahmen führen - etwa zur Ergänzung von Log-Quellen, zur Anpassung von Log-Retentions oder zur Erstellung neuer Parsing- und Erkennungsregeln im SIEM. In Cloud-Umgebungen stellt sich die Frage der Sichtbarkeit neu: Sind Audit-Logs aktiviert? Wie lange bleiben sie verfügbar? Wer hat Zugriff? Können sie im Incidentfall exportiert und analysiert werden?

In der Praxis zeigt sich immer wieder, dass viele Cloud-Umgebungen über Jahre hinweg im Standardzustand betrieben oder nur punktuell angepasst wurden - oft ohne vollständige Dokumentation oder regelmäßige Überprüfung der Logging-Konfiguration. Dabei wird vielfach angenommen, dass alle sicherheitsrelevanten Aktivitäten automatisch protokolliert werden.

Ein Beispiel dafür ist das Unified Audit Log in Microsoft 365: Bis 2023 musste dieses manuell aktiviert werden. Bei Tenants, die vor diesem Zeitraum angelegt wurden, ist diese Konfiguration weiterhin manuell erforderlich. Ohne aktive Audit-Logs fehlen im Incidentfall zentrale Informationen darüber, welche Aktionen ein Angreifer im Tenant durchgeführt hat - etwa das Anlegen neuer Postfächer, das Setzen von Weiterleitungen oder das Einsehen von Dokumenten.

Eine regelmäßige Überprüfung der Log-Aktivierung und -Retention in Cloud-Diensten ist daher unerlässlich, um im Ernstfall auf aussagekräftige Daten zugreifen zu können. Sichtbarkeit ist kein Selbstzweck. Sie ist zentrale Voraussetzung für eine schnelle Identifikation, effektive Eindämmung und gründliche Bereinigung eines Angriffs. Ohne Sichtbarkeit wird Incident Response zur Blindfahrt.

Menschliche Faktoren

Security ist kein Tool, sondern ein Verhalten. Und Verhalten ist trainierbar. Ein entscheidender Teil der Preparation-Phase ist daher die Schulung und Sensibilisierung der Menschen, die im Ernstfall reagieren müssen. Es beginnt bei einfachen Awareness-Maßnahmen, Phishing-Kampagnen, Trainings und Cheat Sheets. Aber es endet nicht dort. Wirkliche Reaktionsfähigkeit entsteht erst durch Übung des Ernstfalls.

Table-Top-Tests, realistische Angriffssimulationen und Red Team Exercises übertragen Theorie in gelebte Praxis. Sie zeigen Schwachstellen auf, bevor ein realer Angreifer sie ausnutzt. Entscheidend ist jedoch, dass diese Übungen nicht isoliert bleiben, sondern systematisch ausgewertet und nachbearbeitet werden.

Dabei stellen sich häufig zentrale Fragen:

- Wie hätte das Red Team Assessment oder der Pentest schneller erkannt werden können?
- Reicht eine Optimierung des vorhandenen EDR oder ist zusätzliche Sichtbarkeit durch ergänzende Logs erforderlich?
- Gibt es definierte Wege, um Unterstützung einzuholen, wenn ein Alarm nicht sicher eingeschätzt werden kann?

Nur wenn sich Teams aktiv mit den Ergebnissen auseinandersetzen und daraus konkrete Verbesserungen ableiten, entsteht ein tatsächlicher Mehrwert für die Incident-Readiness. Ein gutes Zeichen ist es, wenn ein Incident nicht zum ersten Mal „gedacht“ wird. Wenn Abläufe klar sind, Kommunikation funktioniert und Entscheidungen getroffen werden können, ohne erst Freigaben oder Zugänge zu organisieren. Genau das ist Ziel und Ergebnis einer starken Preparation.

Kommunikation im Ausnahmezustand

In der Ruhe liegt die Kraft - aber was, wenn die Kommunikationskanäle gestört sind? Preparation muss auch Szenarien abdecken, in denen klassische IT-Infrastruktur nicht mehr zur Verfügung steht. Wenn Mailserver ausfallen, VPNs kompromittiert sind und Collaboration-Tools nicht erreichbar sind, braucht es Alternativen.

Hier kommen Out-of-Band-Kommunikation, verschlüsselte Messenger, Notfalltelefone oder sogar Papierpläne zum Einsatz. Entscheidend ist nicht die Technik, sondern die Vorbereitung: Wissen alle Beteiligten, wie sie im Ernstfall erreicht werden? Gibt es Backup-Listen, Notfallnummern, klare Eskalationsregeln? Wer im Vorfeld kommuniziert, muss im Ernstfall nicht improvisieren. Und wer sich auf das Versagen vorbereitet, kann in der Krise souverän handeln.


PODCAST
CYBER SECURITY
Basement
In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking“. Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.
Jetzt reinhören
Spotify
Apple Podcast
YouTube Music
amazon music
und noch mehr...

Fazit: Preparation als Kern moderner Sicherheitskultur

Preparation ist mehr als ein Kapitel im NIST-Dokument. Sie ist Ausdruck einer Sicherheitskultur, die Verantwortung ernst nimmt. Wer vorbereitet ist, gewinnt Zeit, Sicherheit und Handlungsfähigkeit. Wer vorbereitet ist, begegnet dem Unvorhersehbaren mit Struktur. Und wer vorbereitet ist, wird aus einem Angriff keine Krise machen.

Preparation beginnt mit Fragen: Sehen wir, was passiert? Haben wir einen vollständigen Überblick über sicherheitsrelevante Ereignisse in unseren Systemen? Welche Use-Cases sind in unseren Security Lösungen konkret implementiert und getestet? Wie zuverlässig funktioniert die Log-Korrelation - sowohl in Echtzeit als auch in der Nachanalyse? Verfügen wir über belastbare Metriken zur Sichtbarkeit - etwa einen vollständigen Überblick über alle Systeme im Netzwerk und deren aktuellen Sicherheitsstatus?

Und nicht zuletzt: Wissen wir, was zu tun ist, wenn ein Incident eintritt - technisch, kommunikativ und operativ? Haben wir das geübt? Wer hier mit Ja antworten kann, hat bereits den ersten Schritt getan. Alle anderen finden in diesem Whitepaper einen Wegweiser, wie sie diesen Schritt gehen. Denn eines ist sicher: Der Ernstfall kommt. Die Frage ist nur, wie vorbereitet du dann bist.

Unser SOC - ohne Kompromisse:

- Automated Response (SOAR)
- Standard Sources
- Cyberaudit
- Incident Response
- suresecure Detection Rules
- Incident Drill
- Customer Success Manager
- Attack Surface Monitoring
- SIEM
- Vulnerability Management
- Security Advisory

Google Security Operations

Google Threat Intelligence

Schlusswort:

Wer glaubt, mit den richtigen Tools auf alles vorbereitet zu sein, irrt. Preparation ist keine Frage von Produkten, sondern von Prinzipien. Keine Konsole, kein Framework und kein Dashboard ersetzt eine Organisation, die weiß, was sie tut - bevor es ernst wird.

Sicherheit entsteht nicht im Alarmfall. Sie entsteht davor. In Strukturen, die tragen. In Logs, die sprechen. In Menschen, die wissen, was zu tun ist. Wer vorbereitet ist, agiert. Wer es nicht ist, reagiert - und verliert dabei oft mehr als nur Zeit.

Weitere Informationen zum Thema:

Podcast-Folge:

Das ist Forensik in meinen Ohren:
Interview mit André

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de