Controlware GmbH

E-Book

The Analyst –
oder wie ich lernte unser Security Operation Center zu lieben

Kontakt: sec-bd@controlware.de

Autor:
Controlware GmbH
Waldstraße 92
63128 Dietzenbach

controlware
communicationssystems

Montagmorgen

… und es ist ein guter Start in die zweite Woche bei meinem neuen Arbeitgeber! Gerade habe ich von einem Kollegen im Marketing einen Link auf ein Excel-Sheet per E-Mail erhalten. Die Beispiele für Werbeaktionen im Sheet sind wirklich gut und ich versuche, diese auch gleich auf mein erstes Projekt anzuwenden. Die E-Mail kam zwar nicht von seiner Firmenadresse, aber das liegt wohl daran, dass der Kollege eigentlich im Urlaub ist.

Eine Stunde später steht eine Kollegin der IT an meinem Schreibtisch und fragt nach, ob ich ein Excel-Sheet über einen Link in einer E-Mail geladen hätte. Betreff und Absender kennt sie bereits. Die Kollegin erklärt mir, dass ich durch das Anklicken des Links Malware im Unternehmen verbreitet habe – aber das sei nun glücklicherweise unter Kontrolle. Bei der Gelegenheit weist Sie mich eindringlich darauf hin, zukünftig keine Makros in Office-Dokumenten zu aktivieren. Irgendwie doch kein so guter Start in die Woche …

Das Security Operation Center

Die Tatsache, dass Benutzer auf Tricks von Angreifern hereinfallen, ist grundsätzlich schlecht. Mit Security Awareness-Programmen kann zwar gegengesteuert werden, aber ganz verhindern lässt es sich nicht. Es ist daher unerlässlich, schnell und effektiv auf Sicherheitsvorfälle zu reagieren. Das Security Operation Center (SOC) war in unserem Beispiel im Hintergrund sofort aktiv:

- Eine Advanced Threat Protection (ATP)-Lösung für Web-Traffic bemerkt den Download des Excel-Sheets und untersucht die Datei in einer Sandbox. In diesem Fall ist klar: Der enthaltene Makro-Code ist schädlich, aber schon am Endpunkt angekommen.
- Der Alarm der Sandbox zeigt bereits, woran eine Infektion erkannt werden kann: Die Malware ruft beim Start eine bestimmte URL auf. Die Logs des Web Gateways offenbaren, dass die Malware-URL vom Client des neuen Mitarbeiters aufgerufen wurde. Die Infektion hat also längst stattgefunden. Kurze Zeit später rufen weitere Clients die URL auf.
- Sowohl die URL als auch die Adresse des Excel-Sheets werden jetzt am Web Gateway blockiert. Die betroffenen Clients werden gesperrt und desinfiziert, damit sie keinen weiteren Schaden im Unternehmensnetzwerk anrichten.
- Ein Malware-Analyst schaut sich das Makro und die nachgeladene Malware genauer an. Sie verbreitet sich selbstständig mit Hilfe einer kürzlich entdeckten Sicherheitslücke. Der Analyst stellt weitere Merkmale fest, mit denen sich infizierte Systeme erkennen lassen.
- Nach diesen Merkmalen wird mit einer Endpoint Detection and Response-Lösung auf allen Clients des Unternehmens gesucht. So soll sichergestellt werden, dass die Infektion komplett eingedämmt ist.

Als eine Art Leitstand für alle sicherheitsrelevanten IT-Services im Unternehmen erkennt das Security Operation Center Bedrohungen frühzeitig und bekämpft diese proaktiv. Alle relevanten Abteilungen werden umgehend eingebunden, Abwehrmaßnahmen definiert und entsprechende Reaktionen koordiniert. Die folgenden Seiten geben einen Überblick der technischen Komponenten in einem typischen SOC und liefern Empfehlungen, welche Schritte beim Aufbau und Betrieb beachtet werden sollten.

Threats und Threat Vectors

Bei unserem Beispiel handelt es sich um einen typischen Angriff auf ein mittelgroßes oder großes Unternehmen. Darüber hinaus gibt es jedoch eine Vielzahl weiterer Möglichkeiten, wie eine Attacke ablaufen kann.

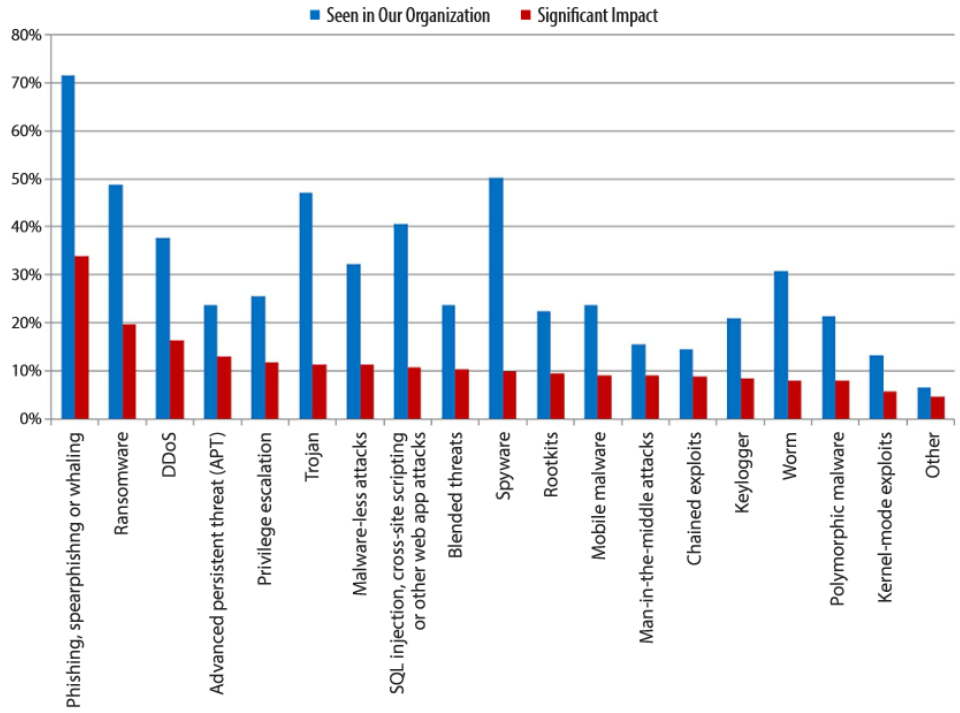
Beflügelt durch den zunehmenden Grad der Digitalisierung und Vernetzung wird sich die Bedrohungslage für Unternehmen in den nächsten Jahren weiter verschärfen. Mögliche Bedrohungen (Threats) reichen von kleineren Ransomware-Angriffen bis hin zu sogenannten Advanced Persistent Threats (APT), die immense Auswirkungen auf die Zukunft eines Unternehmens haben können. Vor allem die Clients der Endbenutzer sind potentiellen Threats ausgesetzt – gleichgültig wie diese mit dem Internet verbunden sind. Die Gründe dafür sind vielfältig. Grundsätzlich lässt sich aber sagen, dass Clients die größte Angriffsfläche bieten und durch die direkte Benutzerinteraktion anfällig für Phishing und andere interaktive Angriffe sind.

Um die aktuellen Bedrohungen für die Unternehmens-IT nachvollziehen zu können, ist es wichtig, zunächst die Terminologie zu verstehen:

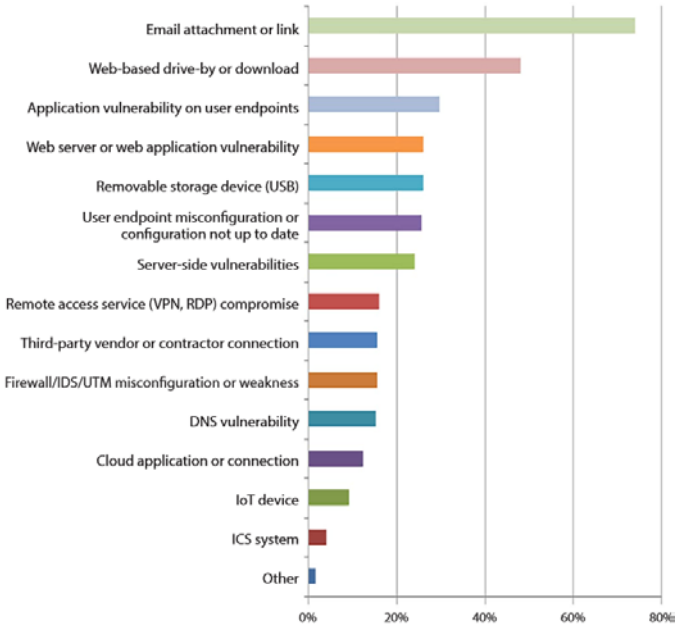
- Ein **Threat** ist eine Sicherheitsbedrohung für die Unternehmens-IT. Ein Threat existiert, wenn Umstände, Fähigkeit, Handlung oder Ereignisse zusammenkommen und daraus resultierend Risiken entstehen.
- Ein **Threat Vector** ist eine Methode, die einen **Threat** nutzt, um zum Ziel zu gelangen.
- Ein Phishing-Angriff stellt beispielsweise einen Threat dar, der wiederum das Medium E-Mail als Threat Vector nutzt.

Das SANS Institute veröffentlicht jedes Jahr eine Studie, in der die aktuelle Bedrohungslage für Unternehmen anhand verschiedener Umfragen erfasst wird. Folgende Grafiken zeigen die Ergebnisse aus dem Jahr 2017:

Threats



Threat Vectors



Quelle *https://www.sans.org/reading-room/whitepapers/Threats/2017-Threat-landscape-survey-users-front-line-37910*

E-Mail und Web scheinen für die Angreifer die beliebtesten Wege in Unternehmen zu sein. Daher ist es absolut notwendig, gerade hier entsprechende Schutzmaßnahmen einzusetzen. Ohne Frage gibt es natürlich auch zahlreiche andere Wege in Unternehmensnetzwerke.

Wie Angriffe ablaufen

Typische Angriffe auf Unternehmen können durch die sogenannte Cyber Kill Chain dargestellt werden. Ein Angriff unterteilt sich dabei in drei Phasen. In jeder Phase gibt es Möglichkeiten, den Angriff zu erkennen und abzuwehren.

In der **Vorbereitungsphase** geht es Angreifern primär darum, Angriffsziele und zugehörige Schwachstellen von außen zu finden. Dabei kann es sich sowohl um Software-Schwachstellen als auch um Fehler in Web-Anwendungen handeln. Es werden passende Exploits ausgewählt oder selbst entwickelt. Ein Lösungsansatz an dieser Stelle ist der Aufbau eines **Vulnerability Management Systems**. Social Engineering-Aktivitäten durch Angreifer sind ebenfalls in diese Phase einzuordnen. Diesen kann durch Anti-Phishing-Lösungen sowie durch Awareness-Schulungen für die Mitarbeiter begegnet werden.

In der **zweiten Phase** findet der eigentliche Einbruch statt. Hier werden beispielsweise präparierte E-Mails an Mitarbeiter im Unternehmen geschickt, um gezielt die vorher ausgewählten Exploits auszuführen und Zugang zum Unternehmensnetzwerk zu erlangen. **Advanced Threat Protection- Lösungen** fokussieren sich in dieser Phase darauf, Infektionen möglichst früh zu erkennen und umgehend zu unterbinden. Diese Lösungen setzen sowohl auf die Threat Vectors Web und E-Mail als auch auf dem Endpoint auf.

Schließlich folgt die **dritte Phase**, in der sich die Angreifer im Netzwerk bewegen, weitere Tools und Backdoors installieren, ihre Rechte ausweiten und zum Beispiel Daten stehlen. Lösungen in dieser Phase sind darauf spezialisiert, Angreifer oder Insider zu erkennen, die sich bereits im Netzwerk befinden, da hier die klassischen Sicherheitslösungen nahezu keinen Schutz mehr bieten. In dieser Phase kommen sowohl **UEBA** (User and Entity Behavior Analytics)-Lösungen auf Basis eines Log- Management-Systems/**SIEM** als auch **NBA**-Lösungen (Network Behavioral Analytics) zur Erkennung von Breaches zum Einsatz. Weiterhin unterstützen **EDR**-Lösungen (Endpoint Detection and Response) bei der Verifizierung und Eindämmung von Infektionen sowie bei der Bestimmung der Infektionsausbreitung im Netzwerk. **Threat Orchestration-**Lösungen bilden das Bindeglied zwischen verschiedenen Lösungen unterschiedlicher Hersteller, um definierte Response-Aktionen zu automatisieren.

Generell empfiehlt sich der Einsatz eines **Log-Managements**, um Logdaten aus verschiedenen Quellen (Security Devices, Netzwerk-Devices, Domain Controller, Benutzer-Aktivitäten u.a.) zentral zu verwalten – unabhängig davon, ob aus Compliance-Anforderungen oder Eigenmotivation. Ein Log-Management bildet auch die Basis für ein **SIEM**-System (Security Information and Event Management), mit dem sich besonders wertvolle Assets auf Basis der Logdaten überwachen lassen. Das Eintreten sicherheitsrelevanter Ereignisse wird über die Definition kritischer Anwendungsfälle, sogenannter Use-Cases, und deren Abbildung durch Korrelation verschiedener Logdaten überwacht.

Technische Bausteine

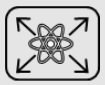
Die technischen Bausteine dienen der Prävention von Sicherheitsvorfällen oder ihrer Entdeckung (Sensorik). Dabei wird oftmals unterschiedliche Sensorik verwendet, um verschiedene Phasen eines Angriffs erkennen zu können. Schließlich sind auch reaktive Bausteine notwendig, um Informationen aktiv zu sammeln, Spuren zu sichern und die Angreifer zu stoppen.

Vulnerability-Management – Probleme früh erkennen und beheben

Patch- und Asset-Management stellen sicher, dass alle aktuellen Updates genutzt werden und, dass kein Server vergessen wird. Soweit die Theorie. In der Praxis sieht es häufig anders aus. Spätestens ab einer bestimmten Netzwerkgröße können Systeme durchaus vergessen werden und manche Updates klemmen einfach. Hier sind Schwachstellen-Scans am Perimeter sinnvoll, um Angreifern die Ziele für den Einstieg in das Unternehmensnetzwerk zu nehmen. Interne Schwachstellen-Scans finden Konfigurationsfehler und entdecken Systeme der Schatten-IT.

Schwachstellen-Scans finden allerdings nur Probleme, beheben diese jedoch noch nicht. Sie müssen regelmäßig durchgeführt werden und sind in einen Prozess zur Priorisierung, Zuweisung von Verantwortlichkeit, Fehlerbehebung und Nachverfolgung einzubinden. Dies wird als Vulnerability-Management bezeichnet. Ein effektives Vulnerability-Management mit internen und externen Scans minimiert die Ansatzpunkte für Angriffe.

Advanced Threat Protection – Mehr als die Erkennung von Standard-Malware

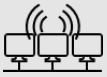


Typische Antiviren-Lösungen suchen signaturbasiert nach Mustern bekannter Malware. Im Gegensatz dazu werden die Inhalte bei Advanced Threat Protection-Lösungen (ATP) in einer virtuellen Umgebung, der Sandbox, automatisiert gestartet. Die Sandbox wird dabei genau beobachtet, um zu erkennen, ob Malware startet – unter anderem durch neu angelegte Dateien, überraschende Netzwerkverbindungen oder andere verdächtige Systemaktivitäten. Auf diese Weise lässt sich auch Malware erkennen, die bisher unbekannt war und zu der demzufolge noch keine Signatur existiert. ATP-Lösungen liefern in der Regel zusätzlich Hinweise, wie ein infiziertes System erkannt werden kann (Indicators of Compromise: IOC).

Werden Web-Sessions mit Hilfe einer ATP-Lösung geschützt, sollte auch der verschlüsselte Web-Traffic untersucht werden. Beim Schutz von Web-Sessions erfolgt außerdem die Alarmierung verzögert: d.h. der Benutzer hat bereits Zugriff auf die verdächtige Datei bevor das Ergebnis der Analyse vorliegt und kann schon eine Infektion auslösen. Ein eingespieltes Betriebsteam ist allerdings durch eine zeitnahe Reaktion auch dann in der

Lage, das Schlimmste zu verhindern. Empfehlenswert ist es, Malware-Analysten hinzuzuziehen, um unklare Ergebnisse zeitnah zu analysieren und zu bewerten. Insgesamt erkennen Advanced Threat Detection-Lösungen Malware zuverlässiger als reine Antiviren-Lösungen und liefern hilfreiche Zusatzinformationen zur Erkennung infizierter Systeme.

Endpoint Detection and Response – Handlungsfähig am Client



Endpoint Detection and Response (EDR)-Lösungen ermöglichen einen effektiven Incident Response-Prozess auf den Endpunkten. Ungewöhnliches Systemverhalten oder Policy-Verstöße werden aufgespürt und es ist eine aktive Suche nach Hinweisen auf Malware möglich (Threat Hunting mit IOCs). Spuren lassen sich sichern, Malware wird je nach Lösung aktiv gestoppt und das System wird in einen sicheren Zustand zurückgesetzt (Containment und Recovery).

Eine Advanced Threat Protection-Lösung ist in der Lage, Hinweise auf Malware zu liefern, nach denen mit Hilfe der Endpoint Detection and Response-Lösung auf allen Endpunkten gesucht wird. Weiterhin können Ergebnisse aus Analysen im Log-Management oder aus SIEM-Systemen für das Threat Hunting verwendet werden. Mit Hilfe von Threat Intelligence Feeds ist es möglich, auf den Endpunkten kontinuierlich nach Anzeichen von Malware zu suchen und entsprechend zu reagieren. Andersherum besteht die Möglichkeit, verdächtige Dateien von Endpunkten direkt an eine Advanced Threat Protection-Lösung zur Analyse zu übergeben. Damit erhalten Bedrohungen auf dem Endpunkt eine bessere Sichtbarkeit – gleichzeitig kann das SOC dort reaktiv eingreifen.

Security Incident & Event Management (SIEM) – Die Steuerungs-zentrale

Heutige IT-Infrastrukturen bestehen aus einem Sammelsurium verschiedenster Komponenten vieler Hersteller. Oftmals werden die Komponenten von unterschiedlichen Abteilungen betrieben und sind auf mehrere Einsatzzwecke fokussiert. Dabei erfolgt die Generierung etlicher Log-Meldungen, die auch sicherheitsrelevante Informationen beinhalten. Ein zentrales Log-Management mit integrierter Intelligenz (SIEM) ermöglicht es, ein umfassendes Bild des IT- Sicherheitslevel darzustellen. So lassen sich Ereignisse (Events) in einen Zusammenhang bringen und analysieren. Darüber hinaus können sogenannte Reputations-Dienste eingebunden werden, um verdächtige Datenkommunikation aufzudecken.

User & Entity Behavioral Analysis (UEBA) – Verhaltensbasierte Analyse

Inzwischen werden traditionelle SIEM-Systeme durch User & Entity Behavioral Analysis-Lösungen (UEBA) ergänzt. Die UEBA-Systeme lernen das Verhalten von Usern und kennen nach einer Lernphase das normale Verhalten der einzelnen User. Eine Risikobewertung (Scoring) des analysierten Verhaltens des betroffenen Users führt bei Überschreitung eines Schwellwertes zu einer Alarmierung. Diese Vorgehensweise steigert die Qualität der Erkennung von Angriffen enorm. Die für die eventuell notwendige Forensik und Gerichtsverwertbarkeit vorliegenden Logdaten existieren weiterhin als Rohdaten signiert im SIEM-Logdatenspeicher. UEBA-Lösungen sind damit in der Lage, die False Positive-Raten gering zu halten und können schneller und effektiver auf die wirklich wichtigen Vorfälle reagieren.

Threat Orchestrierungssoftware – Der automatisierte Dirigent

In der Regel bestehen größere IT-Security-Infrastrukturen aus einer Vielzahl von Komponenten unterschiedlicher Hersteller mit zahlreichen Funktionen, Schnittstellen und APIs. Mit einer sogenannten Threat-Orchestrierungssoftware lässt sich dieses „Chaos" beseitigen.

Eine Threat-Orchestrierungssoftware unterstützt die Security-Analysten durch Automatisierung über Play Books. Die APIs der einzelnen Komponenten werden genutzt, um Informationen zu sammeln und automatisch Aktionen auszuführen. Damit wird die Threat-Orchestrierungssoftware zum zentralen System, über das alle gängigen Arbeitsabläufe gesteuert werden können. Die Bearbeitung der einzelnen Incidents erfolgt über Schnittstellen in das Ticketsystem und wird vom Security Level Management überwacht.

Zusammenspiel der Lösungen

Moderne mehrstufige Angriffe sind generell schwer zu erkennen. Die Angreifer halten sich natürlich nicht an unsere Incident Response-Pläne und nutzen auch Threat Vectors und Schwachstellen, die im Vorfeld nicht bedacht wurden. Dadurch werden nicht alle Elemente der Cyber Kill Chain sichtbar, sondern nur Fragmente davon. Aus diesem Grund ist es nicht ausreichend, zum Beispiel nur den Netzwerkperimeter zu schützen. Es ist unbedingt erforderlich, auch Sensorik zur Erkennung von Angriffen im internen Netzwerk zu betreiben. Darüber hinaus sind forensische und reaktive Tools notwendig, um Alarme zu verifizieren und auf Angriffe effektiv zu reagieren.

Wie Incident Response ablaufen könnte

Die **Advanced Threat Protection** (ATP) löst einen Malware-Alarm auf einem Client aus. Das **Vulnerability Management** informiert darüber, ob der Client überhaupt für den erkannten Exploit verwundbar ist. Daraufhin wird der Client mit dem **Endpoint Detection and Response** System (EDR) näher untersucht. Der Speicher verdächtiger Prozesse und andere Spuren lassen sich zur Analyse sichern. Des Weiteren werden im zentralen **SIEM** Hinweise aus den Logfiles korreliert, um herauszufinden, wie der Angriff ablief und ob weitere Systeme betroffen sind.

Verdächtige URLs, IP- und E-Mail-Adressen aus abonnierter Threat Intelligence und aus eigenen Blacklisten reichern das SIEM-System an. Mit Hilfe von **Threat-Orchestrierung** ist es möglich, automatisiert zu reagieren – zum Beispiel durch sofortiges, automatisches Blocken von Verbindungen an den angebundenen Security-Systemen (Proxy, E-Mail-Server, Firewall). Alternativ kann die Reaktion halbautomatisch über einen Freigabe-Workflow erfolgen.

Die **UEBA-**Lösung ergänzt das SIEM, indem sie das typische Verhalten von Usern erlernt. Auf diese Weise ist die UEBA-Lösung in der Lage, zu alarmieren, wenn vermehrt unübliches Verhalten entdeckt wird. Das Gleiche gilt, wenn ein bestimmtes Angriffsszenario nicht antizipiert wurde, es also keinen Use Case dafür gibt.

It’s the People – Das Security Team

Um den größten Nutzen mit den eingesetzten Security-Lösungen zu erzielen, werden qualifizierte Mitarbeiter benötigt (Cyber Security-Analysten). Diese sollten über unterschiedliches Fachwissen und Erfahrung in folgenden Bereichen verfügen:

- Vorgehen und Techniken von Angreifern und Malware
- Malware-Analyse und Reverse Engineering
- Automatisierung und Orchestrierung
- Betriebssystem, Netzwerk, Perimeter-Schutz, Endpoint-Schutz
- Beurteilung von Sicherheitslücken und Durchführung von Schwachstellenmanagement
- Forensik
- …

Wie viele Security-Mitarbeiter benötigt werden, lässt sich nicht eindeutig beziffern. Wird beispielsweise in einem bestimmten Bereich eine hohe Verfügbarkeit benötigt (z.B. Malware-Analyse), dann müssen entsprechend viele Mitarbeiter mit diesen Fachkenntnissen vorhanden sein. Aufgrund des aktuellen Fachkräftemangels ist es jedoch nicht einfach, Mitarbeiter mit den benötigten Kenntnissen und Erfahrungen zu gewinnen. Wichtig ist hier die Qualität, nicht die Quantität. Ein großes Team bedeutet nicht zwangsläufig, dass effektiv gearbeitet wird. Es kann durchaus sinnvoller sein, ein kleines, kompetentes Team kontinuierlich aufzubauen und dabei nur ein moderates Wachstum an neuen Mitarbeitern anzustreben.

Neue Technologien im Bereich künstlicher Intelligenz und Machine Learning versprechen, Personalmangel zu überbrücken. Unter anderem lassen sich Arbeitsabläufe einzelner Spezialisten mit Hilfe von Threat-Orchestrierungssoftware automatisieren und allen Security-Analysten zur Verfügung stellen. Weiterhin besteht die Möglichkeit, einzelne Themenfelder durch externe Dienstleister abzudecken. Bei digitaler Forensik, Reverse Engineering und Malware-Analyse ist dies gängige Praxis, da die Aufgaben oftmals schwer selbst zu bewerkstelligen sind. Hierbei ist es wichtig, dass die Interaktion mit dem Dienstleister klar geregelt ist und die Abläufe geprobt wurden.

Die Security-Analysten im SOC müssen Fachkenntnisse und Erfahrung mitbringen und sollten folgende Fragen klären, die in der Regel bei einem APT-Alarm in einer Web-Session aufkommen:

- Um welchen Exploit Vector handelt es sich? (Welche Ziel-Applikation? Wie lautet die CVE ID der Schwachstelle?)
- War das Ziel-System verwundbar? (Abgleich mit Schwachstellen-Management)
- Wie kritisch ist das System? (Abgleich GRC-System, Kritikalität der Daten, abhängige Geschäftsprozesse)
- Woher kam der Exploit? (Handelt es sich um ein Exploit Kit? Wird immer der gleiche Exploit ausgeliefert? Besteht dabei eine Abhängigkeit von Quell-IP, Betriebssystem etc.?)
- Was ist in dem Kontext passiert? (Analyse Logdaten, verdächtige Verbindungen, ausgehende Angriffe, nachgeladener Schadcode)
- Was ist die Funktionalität des Exploit und der nachgeladenen Malware? (Analyse des Schadcodes, Ist der Code bekannt oder Reverse Engineering notwendig? Besteht Bezug zu bekannten Malware-Familien oder Cybercrime-Organisationen? Besitzt die Software zusätzliche Funktionalität, z.B. selbstständige Verbreitung? Hinweise zur Erkennung der Malware (IOCs))
- Sind die beteiligten IPs und URLs schon gesperrt und Malware Hashes bekannt? (auf eigene Blacklisten setzen, ggf. den Security-Hersteller informieren)

Montagmorgen – So hätte es auch ausgehen können

Kommen wir erneut auf das Beispiel vom Anfang zurück und stellen uns einen anderen Verlauf vor. Das SOC hätte nicht schlagkräftig und schnell reagiert und die Malware wäre länger unbemerkt geblieben. Nehmen wir weiterhin an, ein konkurrierendes Unternehmen aus einem anderen Land hätte die Malware versendet. Plötzlich scheinen alle unsere guten Ideen auch dem Konkurrenzunternehmen einzufallen. Ausschreibungen verlieren wir immer wieder, weil wir knapp unterboten werden. Unsere Geschäftszahlen verschlechtern sich aufgrund der rückläufigen Umsätze und irgendwann steht der Weiterbestand des Unternehmens auf dem Spiel.

Sicherheitsvorfälle aussitzen und hoffen, dass diese keinen Schaden verursachen, ist keine Option. Falls bisher keine Schäden verzeichnet wurden, könnte dies auch bedeuten, dass die Angreifer noch unbemerkt sind. Wichtig ist, sich im Klaren zu sein, dass technische Security-Lösungen ihr volles Potential nur im Zusammenspiel miteinander entfalten. Optimale Unterstützung bietet hier ein Security Operation Center (SOC) – ein Sicherheitsleitstand. Sind die benötigten Ressourcen (noch) nicht vorhanden, kann Controlware als erfahrener Partner beim Aufbau von SOC/Cyber Defense Center-Strukturen effektiv unterstützen. Darüber besteht die Möglichkeit, alle relevanten technischen Bestandteile als Managed Services zu beziehen – bis zum kompletten „Cyber Defense Center as a Service“.

Kontakt:

Telefon +49 6074 858-00
Telefax +49 6074 858-108
E-Mail: sec-bd@controlware.de
https://www.controlware.de