Sofortmaßnahmen – Dos and Don'ts

Wenn Unternehmen wissen, wie sie sich in den ersten Stunden nach einem Angriff verhalten sollen und wie nicht, können sie das Beste aus der Situation machen. Wer hingegen ohne Plan in blindem Aktionismus handelt, kann die Situation noch verschlimmern.

Von Nadia Meichtry

Ransomwaregruppen geht es in erster Linie um Geld. Zahlt das Opfer kein Lösegeld für die Entschlüsselung der Daten, veröffentlichen die Kriminellen diese im Darknet. Manche Gruppen haben keinerlei Moral und schrecken nicht einmal davor zurück, Krankenhäuser anzugreifen. Die neueste Masche ist das Bedrohen von Patienten durch Swatting: Durch das Vortäuschen falscher Tatsachen, zum Beispiel Bombendrohungen, wird ein großer Polizeieinsatz provoziert, sodass schwer bewaffnete Einsatzkommandos bei den Opfern auftauchen. Das setzt die Krankenhäuser unter Druck, das geforderte Lösegeld zu zahlen (siehe ix.de/z9gh).

Um Schäden und Verluste nach einem Angriff zu begrenzen, ist es daher entscheidend, schnell und richtig zu reagieren. Ein Ransomwareangriff ist leicht zu erkennen – doch leider erst dann, wenn es bereits zu spät ist: Die Dateien sind verschlüsselt und auf den Systemen liegt in der Regel eine Readme-Datei mit der Lösegeldforderung. Ideal wäre es, einen Angriff bereits vor dem Verschlüsseln zu erkennen. Es gibt immer wieder Vorfälle, bei denen der Beginn des Angriffs schon einige Monate zurückliegt und die Angreifer unbemerkt in das Netzwerk vorgedrungen sind – und dann plötzlich die Verschlüsselung aktivieren. Dies lässt jedoch einen gewissen Spielraum für die Erkennung.

Wenn eine Organisation ihre Hausaufgaben gemacht hat und die Good Practices für Prävention und Schutz einhält [1], sorgt ein zentraler Malwarescanner oder ein EDR-System (Endpoint Detection and Response) durch die zahlreichen generierten Alarmmeldungen für die Erkennung. Allerdings muss jemand diese Systeme überwachen und auf die Alarmmeldungen reagieren. Die Schadsoftwareklassifizierungen der Hersteller sind teilweise unverständlich. Systemverwaltern hilft das „Antivirus Event Analysis Cheat Sheet" (siehe ix.de/z9gh), solche Meldungen einzuordnen und etwa bei den Tools Cobalt, Mimikatz oder Seatbelt in der Erkennungsnachricht die Alarmstufe Rot auszulösen.

Auf einen Vorfall kann man richtig oder falsch reagieren. Von den getroffenen Entscheidungen hängt unter Umständen das Überleben der Organisation oder zumindest eine schnelle und möglichst verlustfreie Rückkehr zur Normalität ab.

iX-TRACT

- Falsche Entscheidungen und schlechte Organisation können die Situation nach einem Angriff verschärfen und zu noch mehr Schäden führen.
- Von den Best Practices abzuweichen ist möglich, wenn man die damit verbundenen Risiken berücksichtigt. Das gilt besonders für die Datensicherung.
- Neben den technischen Sofortmaßnahmen dürfen administrative Maßnahmen nicht vergessen werden. Besonderes Augenmerk liegt auf der Dokumentation.

Don'ts – was könnte da schiefgehen?

Was alles schiefgehen kann, haben meine Kollegen und ich während verschiedener Ransomwarevorfälle beobachtet. Die nachfolgenden Punkte haben in Fällen, in denen sie nicht berücksichtigt wurden, zu einer deutlichen Verschärfung der Situation geführt.

In einer Krisensituation wie einer Ransomwareattacke stehen alle unter Druck. Doch gerade dann ist es wichtig, nicht in Panik zu verfallen und Ruhe zu bewahren [2]. Anderenfalls besteht die Gefahr, dass man übereilte und unüberlegte Entscheidungen trifft, die mehr schaden als nützen. Die Menschen sind außerdem so stark involviert, dass sie Gefahr laufen, auszubrennen, wenn sie sich vom Stress überwältigen lassen und sich nicht ausreichend erholen. Deshalb ist es notwendig, in Schichten zu arbeiten – das heißt mit sich ablösenden Teams, die die Arbeit ohne Unterbrechung fortsetzen. Die Ressourcen müssen entsprechend geplant werden. Dazu ist es wichtig, einen Überblick über das Personal zu haben und zu wissen, wer bereits involviert ist, wer zur Verfügung steht et cetera.

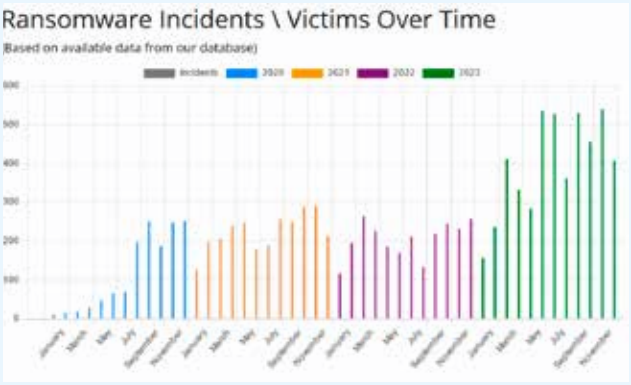
Erschwerend kommt hinzu, dass Angreifer, um unter dem Radar zu bleiben und sich möglichst viel Zeit zu verschaffen, bevorzugt freitags am Tagesende agieren oder sogar außerhalb der Geschäftszeiten. Alarme, die durch ihre Aktivitäten ausgelöst werden, werden so

Einige aufschlussreiche Ransomwarestatistiken

Mehrere Onlinedienste erfassen die verschiedenen Ransomwareangriffe und -opfer und stellen interessante Statistiken zur Verfügung (alle nachfolgend genannten Dienste sind über ix.de/z9gh zu finden). Ransom-DB etwa bildet die Anzahl der Opfer und Vorfälle pro Ransomwaregruppe im Zeitverlauf ab (siehe Abbildung 1).

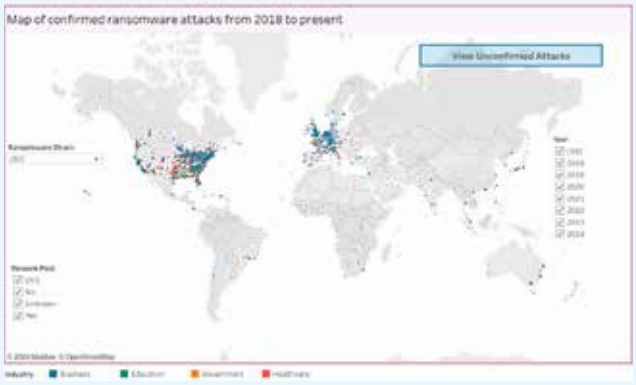
Die Website Ransomwhe.re stellt die Anzahl und Höhe der Zahlungen pro Ransomwarefamilie dar. Die Anzahl der Opfer pro Ransomwaregruppe und Land findet sich im Ransom.Wiki. RansomLook informiert über die Häufigkeit der Veröffentlichungen nach Ransomwaregruppen im Zeitverlauf (Anzahl der gestohlenen Datensätze mit Datum und Tätergruppe).

Die Anzahl der Opfer/Vorfälle und betroffene Branchen nach Ländern sowie die aktivsten Ransomwaregruppen kann man bei Ransomlooker nachschlagen. Und schließlich bietet Comparitech Map einen vergleichenden Überblick über die Anzahl der Angriffe pro Monat nach betroffenem Gewerbe, die durchschnittliche Höhe der Lösegeldforderungen pro Branche und die Anzahl der Angriffe pro Ransomwaregruppe (Abbildung 2).



Anhand der Ransom-DB lässt sich die Entwicklung der Ransomware-Incidents in den letzten Jahren (beginnend 2020) verfolgen (Abb. 1).

Quelle: ransom-db.com



Lässt man sich bei Comparitech Map alle Vorfälle der letzten Jahre in allen Ländern anzeigen, bietet sich ein erschreckendes Bild (Abb. 2).

nicht unbedingt zeitnah bemerkt. Die Verantwortlichen sind möglicherweise nicht mehr erreichbar und die Eskalation verzögert sich, sodass der externe Incident-Response-Partner erst spät eingeschaltet wird. Es kann also einige Zeit dauern, bis die richtigen Personen ins Boot geholt sind. Das bedeutet, man muss selbst am Freitag kurz vor Feierabend noch auf kritische Alarme reagieren können. Es gibt Möglichkeiten, außerhalb der Bürozeiten und damit am Wochenende informiert zu werden, beispielsweise per E-Mail (wie man diese Incident-Benachrichtigungen einstellt, beschreibt ein Microsoft-Artikel; siehe ix.de/z9gh). So werden kritische Alarme nicht erst am Montagmorgen erkannt.

Konkurrierende Interessen koordinieren

Viele unterschätzen die Tatsache, dass große Cybervorfälle wie ein Ransomwareangriff nicht nur ein Problem der IT-Abteilung sind. Vielmehr müssen alle – Geschäftsleitung, höheres Management, Datenschutzbeauftragte, Rechtsdienst und so weiter – beteiligt sein und klar definierte Rollen und Aufgaben haben, damit alles so reibungslos wie möglich abläuft. Allerdings gibt es widersprüchliche Ziele und Zeitpläne zwischen den verschiedenen Beteiligten: Zum Beispiel wollen sich die IT-Spezialisten auf den Wiederaufbau konzentrieren, die Incident Responder wollen Daten sichern und Details zum Geschehen sammeln, das Management will so schnell wie möglich Informationen für die Berichterstattung und die Kommunikation mit den Partnern haben und vor allem den Betrieb wieder aufnehmen.

Daher ist es wichtig, einen Plan zu erstellen, der beschreibt, wer was wann zu tun hat. Ohne klare Führung und Organisation geht in einer solchen chaotischen Situation viel Zeit verloren. Die Einheitlichkeit der Vorfallsbehandlung sollte durch einen einzigen Verantwortlichen oder durch eine klare Abgrenzung der Verantwortungsbereiche gewährleistet werden. Aus diesem Grund ist die Rolle eines Incident Managers erforderlich, der als Koordinator und zentraler Ansprechpartner in einem solchen Störfall fungiert [2].

Kommunizieren im Krisenfall

In diesem Zusammenhang ist auch auf die Kommunikation zu achten [1]. Es kann zu Problemen kommen, wenn man zu wenig kommuniziert – oder umgekehrt, wenn zu viele Informationen preisgegeben werden. Im ersten Fall können die Mitarbeitenden verunsichert und überfordert sein und Stakeholder misstrauisch werden, insbesondere wenn sie von Dritten, etwa aus Medienberichten, erfahren, dass ein Angriff stattgefunden hat. Im zweiten Fall kann das Offenlegen von zu vielen Informationen die Aufmerksamkeit der Angreifer erregen. Das kann dazu führen, dass sich der Vorfall verschlimmert oder es zu einem weiteren Vorfall kommt. Beides ist also kontraproduktiv. Hier gilt es, die richtige Balance zu finden. Weitere Empfehlungen zur Kommunikation gibt das neuseeländische CERT in seinem Blogbeitrag (siehe ix.de/z9gh).

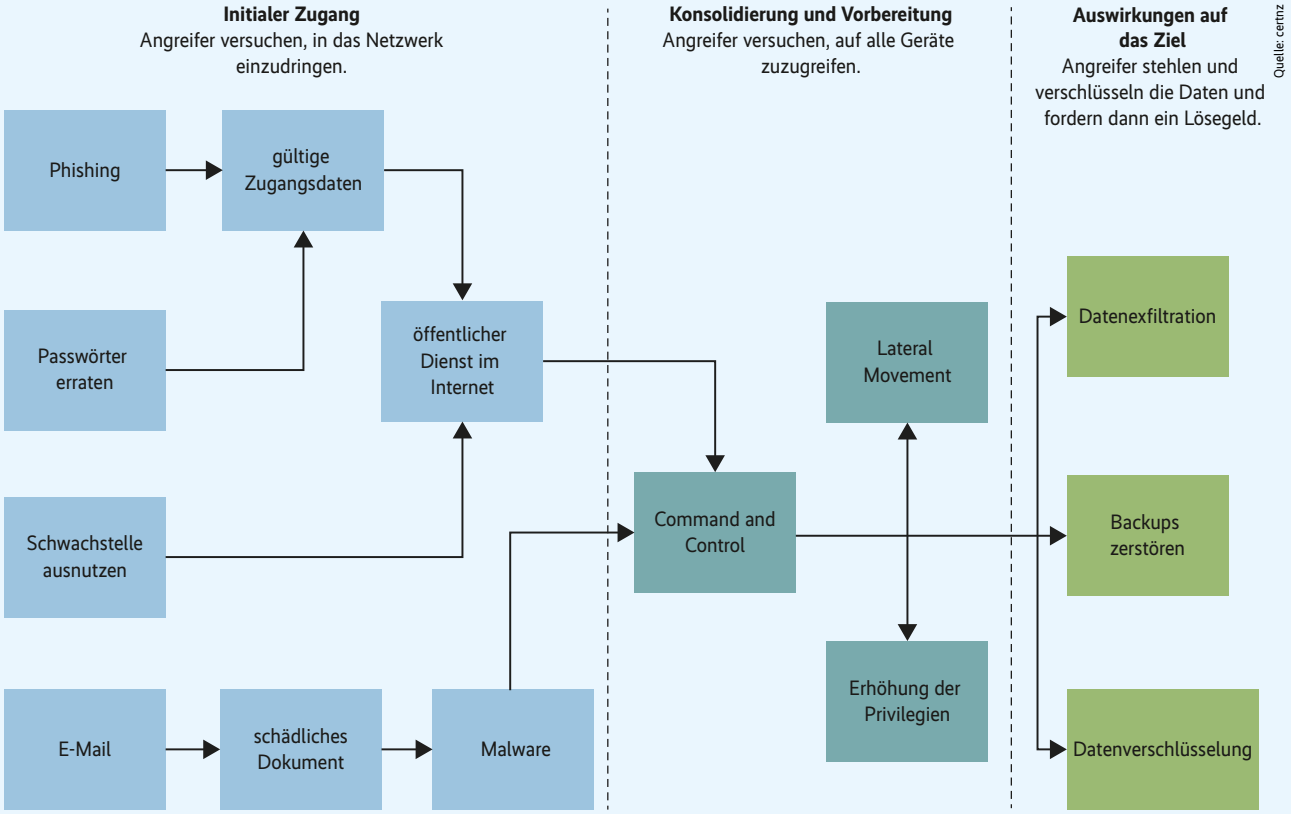
Ein weiterer Punkt, der oft vergessen wird, ist die Informations- und Meldepflicht, sowohl gegenüber den Stakeholdern als auch gegenüber den Behörden. Hierfür gibt es oft sehr kurze Fristen (beispielsweise 72 Stunden für die DSGVO). Die Nichteinhaltung dieser Fristen kann zu Bußgeldern führen. Es ist nicht angenehm, sich als Opfer zu bekennen, aber es ist notwendig. Dies sollte über die Rechts- und Datenschutzabteilung erfolgen. Fachliche Unterstützung ist auch hier unerlässlich [2, 3].

Ein zusätzliches Problem ist, wenn man beim Wiederherstellen übereifrig

Ablauf eines Ransomwareangriffs

Um zu verstehen, wie man am besten auf einen Ransomwareangriff reagieren und sich verteidigen kann, ist es wichtig, seinen genauen Ablauf zu kennen. Das neuseeländische CERT (Computer Emergency Response Team) hat eine Grafik erstellt, die die verschiedenen Phasen vom ersten Zugriff bis zu den Auswirkungen für die Opfer veranschaulicht (siehe Abbildung 3).

In diesem Zusammenhang ist auch die bekannte Angriffsdatenbank ATT&CK-Framework von MITRE hilfreich, um einen Ransomwareangriff zu rekonstruieren. Darüber hinaus stellen die MITRE-Sammlungen MITRE D3FEND, RE&CT und ENGAGE weitere Hilfestellungen, Gegenmaßnahmen und Handlungsanweisungen zur Verfügung (alle sind über ix.de/z9gh zu finden).



Nur wer die einzelnen Phasen eines Ransomwareangriffs kennt, kann eine Verteidigungsstrategie planen (Abb. 3).

und ohne Konzept vorgeht. Manche Systeme werden einfach so aus Backups wiederhergestellt, ohne den Zeitpunkt des Angriffs und die Sauberkeit des Backups zu überprüfen und ohne in der Umgebung nach weiteren kompromittierten Systemen zu suchen. Besonders wenn der Beginn des Angriffs lange zurückliegt, ist es wahrscheinlich, dass auch die Backups infiziert sind. In einigen Fällen ist es nicht möglich festzustellen, wann die Angreifer eingedrungen sind, weil die Logs nicht weit genug zurückreichen. Da die Systeme weiterlaufen, werden die Protokolle einfach überschrieben, weil sie nur eine begrenzte Größe haben.

Des Weiteren ist der Verlust von Daten für die Analyse umso größer, je später die Spezialisten eingebunden werden. So kann es passieren, dass Systeme zu einem späteren Zeitpunkt erneut infiziert werden, weil die Verteidiger eines der infizierten Systeme übersehen haben oder ein System nicht richtig bereinigt und es wieder in Betrieb genommen haben. Ein von WannaCry betroffenes Unternehmen meldete sich ein Jahr später erneut, weil es mit derselben Schadsoftware infiziert worden war. Es ist daher wichtig, keinen Schritt im Incident-Response-Prozess auszulassen.

Maybes – wenn Best Practice nicht immer möglich ist

Gerade bei Cybervorfällen, in denen vor allem die Zeit und die schnelle Reaktion von zentraler Bedeutung sind, kann es vorkommen, dass Best Practices nicht immer eingehalten werden können.

Best Practice in der Eindämmungsphase wäre, die Systeme zu isolieren, aber nicht herunterzufahren, um die volatilen Daten wie Arbeitsspeicherdaten, die beim Herunterfahren verloren gehen, noch für die Analyse zu sichern. Da aber Mitarbeitende meistens nicht wissen, was es bedeutet, ein System vom Netzwerk zu isolieren, könnten sie die Systeme dennoch herunterfahren. Nicht volatile Daten wie Festplatteninhalte können trotzdem gesichert werden.

Manchmal ist es unumgänglich, sich mit einem privilegierten Konto auf einem möglicherweise infizierten System anzumelden. Dieses Risiko sollte man in Ausnahmefällen jedoch eingehen, um Daten zu sichern, die für die Analyse besonders relevant sind. Verteidiger sollten allerdings darauf achten, im Idealfall nur das lokale Administratorkonto zu verwenden, um eine Kompromittierung des Domänenadministrators zu verhindern (auch wenn der Domänenadmin in den meisten Fällen bereits kompromittiert ist). Das verwendete Konto muss dann

als kompromittiert betrachtet und das Passwort unbedingt zurückgesetzt werden [2].

Daten nach Priorität sichern

Bei der Datensicherung verlangen die Best Practices der klassischen IT-forensischen Analyse, die Reihenfolge je nach Volatilität einzuhalten, zum Beispiel sollte man den Arbeitsspeicher vor der Festplatte sichern, die eins zu eins abgebildet werden sollte. Bei einem Ransomwarevorfall ist dies jedoch nicht praktikabel, da es Hunderte infizierter Systeme geben kann und es unrealistisch ist, alle ordnungsgemäß zu sichern. Daher wird in solchen Fällen oftmals eine Triage durchgeführt, um sich auf die für die Analyse relevantesten Artefakte und Systeme zu konzentrieren. Konzept und Durchführung einer Triage werden an anderer Stelle in diesem Heft erläutert.

Gerade bei Ransomwarevorfällen werden oft ganze Systemlandschaften – insbesondere Clients – neu aufgesetzt und installiert. In großen Unternehmen kann dies bei Tausenden Clients jedoch schnell zu einem exorbitanten Aufwand führen. Daher wird oftmals nach einer effizienteren Abkürzung gesucht, in der man versucht, die Systeme zu bereinigen.

Mit dem Bereinigen eines zuvor kompromittierten Systems kann meist nicht mit hundertprozentiger Sicherheit gesagt werden, dass nicht doch noch irgendwo Schadsoftware oder Hintertüren lauern. Es ist daher umso wichtiger, sich eine gute Bereinigungsstrategie zurechtzulegen, die sicherstellt, dass keine Systeme neu infiziert werden. Als Wiederherstellungsstrategie wird empfohlen, eine Testumgebung und eine saubere Umgebung einzurichten, die von der kompromittierten Umgebung isoliert sind und auch keine Verbindungen untereinander haben. Die Testumgebung wird als DMZ (Demilitarized Zone) zwischen der kompromittierten und der sauberen Umgebung betrieben.

In der Testumgebung werden die Systeme auf IOCs (Indicators of Compromise) überprüft. Finden sich solche Hinweise auf eine Kompromittierung, ist eine Neuinstallation des Systems das Beste. Wenn ein Backup verfügbar ist, wird es getestet und dann eingespielt. Ist eine Neuinstallation nicht möglich, wird das System bereinigt, das heißt, die gefundenen IOCs werden entfernt. In der sauberen Umgebung werden die Systeme verbunden, nachdem sie als sauber und sicher eingestuft wurden. Hier ist dann eine starke Überwachung (über EDR et cetera) besonders wichtig. Werden diese Umgebungen nicht gut kontrolliert oder wird ein System nicht ausreichend bereinigt, gelangt dadurch ein kompromittiertes System in die saubere Umgebung, kompromittiert diese und man kann wieder von vorne beginnen.

Dos – reagieren, aber diesmal richtig

Der erste Schritt zur Schadensbegrenzung besteht darin, den Zugang zur Infrastruktur und zu den Systemen für die Angreifer zu sperren, um ihre Aktivitäten zu blockieren. Sind die Eindringlinge noch dabei, Daten zu exportieren, müssen sie auch daran gehindert werden. Dazu ist es wichtig, die infizierten Systeme vom Netzwerk zu trennen. Bei physischen Geräten geschieht dies durch Ziehen des Netzwerkkabels, bei virtualisierten Systemen durch Entfernen oder Deaktivieren der virtuellen Netzwerkkarte. Isolation kann auch durch eine EDR-Lösung erfolgen.

Es ist jedoch im Voraus zu überlegen, welche Folgen es hat, wenn etwa der einzige Domänencontroller oder Mailserver isoliert wird. Zusätzlich muss man besonders wichtige Systeme wie die Backup-Server schützen. Auf diese Infrastruktur darf es von

anderen Systemen keinen Zugriff mehr geben, denn ihre Infektion oder Zerstörung erschwert die Rückkehr zum Normalbetrieb erheblich. Diese Systeme müssen daher in ein anderes Netzwerk verlagert und so isoliert werden.

Generell sollte die Kommunikation vom und zum Internet so stark wie möglich eingeschränkt werden. Im Idealfall können Mitarbeiter weiterarbeiten, aber das Risiko eines Zugriffs ist minimiert. Aus dem Internet erreichbare Dienste sollten daher soweit möglich heruntergefahren oder gestoppt werden. Dabei ist darauf zu achten, dass die Verbindung zum EDR-System nicht unterbrochen wird. Der E-Mail-Verkehr kann auf dem E-Mail-Server noch auf bestimmten Ports zugelassen werden und die Kommunikation vom LAN ins WAN über HTTPS freigeschaltet werden, sodass ein Notbetrieb sichergestellt ist und die Mitarbeitenden reduziert arbeiten können.

Beobachten, was im Netzwerk passiert

Parallel dazu müssen die Verteidiger Visibilität schaffen, um die Situation besser zu verstehen und vor allem das Ausmaß der Infektion zu bestimmen. Dies können sie durch verschiedene Sensoren (EDR, NDR – Network Detection and Response, IDS, IPS, Forensiktool Velociraptor) erreichen, die sie an einigen Stellen im Netzwerk platzieren. Diese Sensoren erlauben es, Aktivitäten festzustellen und darauf zu reagieren; dazu müssen sie scharfgeschaltet werden. Infizierte Systeme, die man so findet, sind unverzüglich zu isolieren.

Ebenso müssen die IOCs festgestellt und anschließend blockiert werden. Dazu müssen Verteidiger IOC-Scans mit Werkzeugen wie Yara oder Thor Lite (siehe ix.de/z9gh) auf allen Geräten durchführen. Unter Last können allerdings einige Systeme (zum Beispiel SANs) ausfallen. Zu den IOCs gehören die Kommunikation mit dem Command-and-Control-Server (IP-Adressen, Domäne), die URLs, die zum Download der Schadsoftware kontaktiert wurden, die Hashwerte der Schadsoftware und alle weiteren Artefakte. Domänen und IP-Adressen lassen sich beispielsweise auf der Firewall blockieren. Die Hashwerte der Schadsoftware [4] kann der Malwarescanner an alle Systeme verteilen, die sie dort blockieren.

Ziel ist es weiterhin, den Angreifer auf Distanz zu halten. Dies ist besonders dann wichtig, wenn der Normalzustand und alle Verbindungen wiederhergestellt sind. Dazu empfiehlt es sich, Sicherheitsfeeds und Blockierlisten in die Geräte am Perimeter – wie Firewalls – einzuspeisen. Beispiele, von denen einige kostenpflichtig sind, sind Feodo Tracker und ThreatFox von Abuse.ch, Spamhaus, TOR-Knoten, Greynoise und AbuseIPDB (alle Links unter ix.de/z9gh).

Darüber hinaus sollte man alle Konten, die als kompromittiert gelten, vorübergehend deaktivieren oder sperren, um den Angreifern den Zugang zu verwehren und sie an der weiteren Ausbreitung zu hindern, falls sie sich noch in der Infrastruktur befinden. Anschließend sollte man alle Passwörter koordiniert zurücksetzen. Passwörter aller Administratoren im Active Directory, Dienstkonten sowie der Kerberos-Vertrauensanker krbtgt dürfen nicht vergessen werden. Der Vorgang für Kerberos muss nach zehn Stunden wiederholt werden, um sicherzustellen, dass keine vor der Kompromittierung ausgestellten und mit dem Kerberos-Konto signierten Ticket Granting Tickets (TGT) eine Authentifizierung innerhalb der Domäne ermöglichen (siehe ix.de/z9gh). Da die maximale Lebensdauer eines TGT zehn Stunden beträgt, ist der Reset nach dieser Zeitspanne zu wiederholen.

Zeitnahe Analyse ermöglicht Schutzmaßnahmen

Trotz Zeitkritikalität sollte man die Analyse des Angriffs auf keinen Fall vernachlässigen. Durch das Untersuchen verschiedener Artefakte und Systeme werden IOCs identifiziert, die überwacht und blockiert werden können. Darüber hinaus ist die Bestimmung des Nullpatienten und des Einfallstors sehr wichtig, um weitere geeignete Schutzmaßnahmen ergreifen zu können – insbesondere auch, um eine zukünftige Reinfektion zu vermeiden. Das Herausfinden des Zeitpunktes des initialen Zugangs ist ebenfalls von zentraler Bedeutung, um das richtige Backup fürs Wiederherstellen zu wählen.

In diesem Zusammenhang ist die Datensicherung relevant. Virtuelle Systeme lassen sich über Snapshots sichern, besonders wichtig sind der Domänencontroller und der Nullpatient. Neben den Logs der internen Systeme und der Schutzsysteme, mit denen man die Ausbreitung innerhalb des Netzwerks bestimmen oder den Nullpatienten finden kann, sollten auch Logs der Geräte am Perimeter (Firewall, VPN et cetera) gesichert werden, da dort möglicherweise der Eintrittspunkt gefunden werden kann.

Auch ein Schwachstellenscan [7] oder Audit der Active-Directory-Konfiguration [8] kann für die Analyse hilfreich sein. Zumindest können die Verteidiger

Auf den Ernstfall vorbereiten

Je besser man auf einen Vorfall wie Ransomware vorbereitet ist, desto schneller lässt er sich bewältigen. Die folgenden Dokumente sollte jedes Unternehmen erstellen und in der Schublade liegen haben.

- Kontaktliste: enthält die Kontaktdaten der verschiedenen Beteiligten und Stellvertreter.
- Incident-Response-Plan: legt die Verantwortlichkeiten, Zuständigkeiten und Aufgaben der einzelnen Beteiligten fest.
- Playbook/Checkliste: definiert die Vorgehensweise und zusätzliche Maßnahmen für ein bestimmtes Angriffsszenario, etwa Ransomware.
- Inventar: versammelt und beschreibt alle Assets und ihre Eigenschaften (Typ, Version, Standort und so weiter).
- Netzplan: stellt alle Komponenten des Netzes und ihre Verbindungen grafisch dar.
- Wiederherstellungsplan: beschreibt die verschiedenen Möglichkeiten und Strategien zur Wiederherstellung der Systeme.
- Kommunikationsplan: legt fest, wie und mit wem kommuniziert werden soll sowie Zeitplan und Ablauf der Kommunikation. Dazu können Erklärungen für gängige Szenarien vorbereitet werden.
- Insbesondere bei einem Ransomwarevorfall gilt es, eine Strategie bei Erpressung zu überlegen, wo untereinander abgestimmt werden soll, wie mit Lösegeldforderungen und Datenveröffentlichung umzugehen ist und gegebenenfalls wie Kryptowährungen wie Bitcoins beschafft werden könnten.

Diese Dokumente sollten regelmäßig getestet und angepasst werden. Eine gute Möglichkeit hierfür sind Tabletop-Übungen mit allen Beteiligten.

den externen IP-Bereich mit Onlinediensten wie Shodan oder Censys (siehe ix.de/z9gh) überprüfen, um die exponierten, von außen erreichbaren Systeme und damit die Angriffsfläche zu ermitteln [9]. Auf diese Weise lassen sich oftmals weitere Indizien zum möglichen Angriffshergang identifizieren, indem Schwachstellen oder Fehler in der Konfiguration entdeckt werden.

Mitschreiben, wer was macht

Im Falle eines Ransomwarevorfalls sollte man nicht nur technische, sondern auch administrative Maßnahmen unverzüglich in die Wege leiten.

Der erste Aspekt betrifft die Dokumentation und hier generell eine gute Nachverfolgbarkeit aller anstehenden Aufgaben. Für ein gutes Krisenmanagement ist dies besonders wichtig. Erfasst werden sollten alle bereits bekannten Informationen wie betroffene Systeme, Artefakte, alle bereits umgesetzten und geplanten Maßnahmen, wer bereits informiert wurde, wer noch zu informieren ist et cetera. Bereits vorhandene Dokumente wie Netzwerkplan und Asset-Inventar sollten ebenfalls den Incident-Response-Spezialisten zur Verfügung gestellt werden. Die Dokumentation ist auch noch im Nachhinein hilfreich, um aus dem Vorfall, den gemachten Fehlern und dem, was gut gelaufen ist, zu lernen und damit die Prozesse zu verbessern.

Ein weiterer Punkt ist, dass viele Unternehmen noch nie einen Vorfall erlebt haben und daher über kein oder zu wenig Know-how verfügen. Dies ist bei einem Ransomwarevorfall und den in sehr kurzer Zeit zu treffenden sehr kritischen Entscheidungen besonders wichtig. Beispielsweise muss die Unternehmensführung schnell entscheiden, ob sie das Lösegeld bezahlt oder nicht, da der Countdown der Angreifer läuft. Hinzu kommt, dass Kryptowährungen wie Bitcoin komplex und zeitaufwendig zu beschaffen sind. Strafverfolgungsbehörden und viele Incident-Response-Dienstleister empfehlen das Zahlen von Lösegeld in der Regel nicht, da es häufig nicht zum gewünschten Erfolg führt und überdies das Geschäftsmodell Erpressung am Leben erhält. Manche Unternehmen sehen für sich jedoch keine andere Lösung.

Unabhängig von der Lösegeldzahlung ist zu überlegen, ob man mit den Angreifern in Kontakt treten möchte, um eventuell weitere Informationen zu erhalten oder Zeit zu gewinnen. Wird auf diese Weise ein Entschlüsselungsprogramm ausgehandelt oder ist bereits eine solche Software frei im Internet verfügbar, muss über eine Wiederherstellungsstrategie nachgedacht werden. Daher empfiehlt es sich, nicht alleine zu handeln, sondern Expertenhilfe in Anspruch zu nehmen.

Einige Tipps zur Protokollierung

Ohne Logs ist die Analyse wesentlich schwieriger, da wichtige Informationen fehlen. Um einen Angriff so detailliert wie möglich rekonstruieren zu können, ist es daher entscheidend, dass Logs vorhanden und richtig konfiguriert sind [5, 6].

Folgende Punkte sind besonders empfehlenswert:

- Größe der Logs erhöhen, damit benötigte Informationen nicht vorher überschrieben werden.
- Benötigte Logs und Ereignisse aktivieren. What2log bietet die Option, ein Skript zur Aktivierung der gewünschten Logs auf verschiedenen Plattformen zu erstellen.
- Windows-Systemdienst Sysmon zum Überwachen und Protokollieren von Systemaktivitäten im Windows-Ereignisprotokoll einsetzen.
- Logs wenn möglich zentral an einem Ort ablegen.

Weiterführende Informationen und Hilfestellungen zu Logkonfigurationen finden sich in den Cheat Sheets bei Malware Archaeology, in den Logging-Empfehlungen des BSI und in den Monitoringhinweisen von Microsoft (alle Links siehe ix.de/z9gh).

Empfehlungen von Behörden

Um bei einem Ransomwarevorfall richtig reagieren zu können, geben auch Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die US-amerikanische Cybersecurity & Infrastructure Security Agency (CISA) die vorgestellten Sofortmaßnahmen vor, außerdem weitere wertvolle Präventions- und Schutzmaßnahmen gegen Ransomwareangriffe.

Die Sicherung der Daten durch Offline-Backups und regelmäßige Wiederherstellungstests gehören zu den wichtigsten Maßnahmen gegen Ransomware [1]. So kann sichergestellt werden, dass die Daten auch nach einer Verschlüsselung noch verfügbar sind.

Darüber hinaus empfiehlt es sich, die von Ransomware häufig genutzten Einfallstore zu schließen oder auf ein Minimum zu reduzieren. Dazu gehört die Ausnutzung von Schwachstellen. Elementar ist es, die eigene Angriffsfläche zu kennen, regelmäßig Schwachstellenscans durchzuführen und vor allem die unterschiedliche Software, Dienste und Geräte auf dem neuesten Stand zu halten. Ein weiterer häufiger verwendeter Einstiegspunkt für Ransomware sind Phishingmails. Mitarbeitende sollten im Umgang damit geschult und sensibilisiert, Makros deaktiviert und eine Zwei-Faktor-Authentisierung implementiert werden. Nicht zuletzt sollten Fernzugriffe wie RDP oder VPN abgesichert werden, da kompromittierte Zugänge ebenfalls zu den Eintrittsvektoren für Ransomware zählen. (ur@ix.de)

Quellen

[1] Inés Atug, Daniel Jedecke; Ransomware-Angriffsmuster und der Schutz dagegen; iX 3/2022, S. 40

[2] Enno Ewers, Martin Junghans; Erste Hilfe nach einem Hackereinbruch; iX 10/2019, S. 46

[3] Tobias Haar; Rechtsfragen zu Ransomware-Attacken; iX 3/2022, S. 56

[4] Nadia Meichtry, Fabian Murer, Tabea Nordieker; Malware-Analyse per OSINT und Sandbox; iX 3/2023, S. 122

[5] Fabian Murer; Incident Response und Forensik – Angreifer durch Logs enttarnen; iX 8/2021, S. 94

[6] Fabian Murer; Forensik und Logging im Azure AD; iX 6/2022, S. 112

[7] Stephan Brandt; Sich selbst hacken: Scannen der eigenen Systeme; iX 8/2023, S. 40

[8] Verschiedene Informationsseiten zu Ransomware, nützliche Tools, Dienste und Hilfeseiten sind über ix.de/z9gh zu finden.

NADIA MEICHTRY

ist Digital-Forensics- und Incident-Response-Spezialistin bei der Oneconsult AG. Sie unterstützt bei der Bewältigung und Untersuchung von Cybervorfällen.