WithSecure™ Countercept präsentiert

Die Kunst der perfekten First Response

Cyberrisiken schneller erkennen, optimal reagieren, Auswirkungen minimieren

Mehmet Surmeli

Senior Incident Response Consultant

John Rogers

Senior Incident Response Consultant

Joani Green

Managing Consultant, Incident Response

James Dorgan

Senior Threat Hunter, Continuous Improvement Lead

WITH secure

Die First Response entscheidet

Trotz hoher Investitionen in Cybersicherheit sind die Unternehmen immer noch unterlegen im Kampf gegen Angreifer, die sich immer weiter anpassen. Die geschäftlichen Auswirkungen eines erfolgreichen Angriffs sind oft beträchtlich und nicht zu verbergen, vielfach ziehen sie weitere Folgen für die Gesellschaft nach sich – ein eiskalter Moment der Wahrheit für jedes Unternehmen. So weit sollte es nicht kommen.

Sicherheitskontrollen versagen, weil Unternehmen nicht im richtigen Moment reagieren. Die Reaktion sollte einen Angriff in dem Augenblick abwehren, in dem er stattfindet, damit das Geschäft nicht beeinträchtigt wird. Allzu oft kommt die Reaktion aber zu spät und in Gestalt einer langwierigen, kostspieligen Wiederherstellung nach einem erfolgreichen Angriff.

Wenn Unternehmen ihre Aufmerksamkeit auf Erkennung und Wiederherstellung statt auf Erkennung und echte Reaktion richten, verpassen sie die entscheidende Gelegenheit, zu reagieren, bevor das Geschäft ernsthaften Schaden nimmt.

Die gute Nachricht ist, dass sich ein Großteil der Folgen abwenden lässt, indem man mit dem Zeitpunkt des Reaktionsbeginns näher an den Moment der Entdeckung rückt. Eine entschlossene Erstreaktion verringert das sehr reale Geschäftsrisiko eines schwerwiegenden Cybersicherheitsvorfalls drastisch.

In diesem Paper erklären wir, woher die Reaktionsverzögerungen kommen und warum die Minimierung der geschäftlichen Auswirkungen und nicht die Geschwindigkeit der Reaktion das Maß des Erfolgs sein sollte. Schließlich werden wir uns ansehen, warum dynamische Ansätze, die das richtige Timing, menschliches Fachwissen und starke Technologie kombinieren, das ergeben, was wir eine starke First Response nennen.

Dieser Report beruht auf den praktischen Erfahrungen der Experten aus den Incident-Response-Teams und den Detection-and- Response-Teams von WithSecure™.

Neue Motive führen zu mehr Angriffen, die mehr Schaden anrichten

In den letzten Jahren hat sich die Herangehensweise der Angreifer grundlegend geändert und dazu geführt, dass die Angriffe an Volumen und Schweregrad zugenommen haben. Angesichts dessen haben sich die Sicherheitskontrollen vieler Unternehmen – von kleinen Firmen bis hin zu Großkonzernen – als völlig unzureichend erwiesen.

Einer der größten Treiber dieser Entwicklung ist: Geld.

Erfolg ermuntert zur Nachahmung. Und erpresserische Cybersicherheitsangriffe, wie sie in den Schlagzeilen stehen, können den Angreifern beträchtliche Gewinne bescheren. Folglich ist die Zahl der Bedrohungsakteure, die an dieser Art von Attacken beteiligt sind, in die Höhe geschnellt, und die Sparte hat auch Angreifer angezogen, die sich zuvor auf Spionage verlegt hatten. Verizon konstatiert in seinem Data Breach Investigations Report 2020 (mit Beiträgen von WithSecure™), dass 86 % der Verstöße, zu denen Daten vorliegen, finanziell motiviert waren, während nur ein Zehntel mit Spionage in Verbindung gebracht wird. Die 2021er Ausgabe des Reports zeigt, dass dieser Trend sich noch einmal verstärkt hat.

Ein Problem nicht nur für große Fische

Dass Bedrohungsakteure sich auf finanziell verlockende Erpressungsangriffe verlegen, hat zur Folge, dass die Liste der potenziellen Opfer sehr viel länger geworden ist; zwar hat nicht jedes Unternehmen Erfindungen und anderes geistiges Eigentum oder streng geheime Informationen zu hüten, aber kaum ein Unternehmen lebt ohne das Risiko einer Erpressung.

Anders gesagt: Das Problem betrifft keineswegs nur kapitalstarke, profilierte Unternehmen.

Einem Coveware-Report zufolge hatten die Unternehmen, die im letzten Quartal 2020 von Ransomware-Angriffen betroffen waren, im Durchschnitt nur 234 Mitarbeiter. 35,7 % der Attacken betrafen Organisationen mit 101 bis 1000 Beschäftigten.

Sich in der Herde zu verstecken und auf „Security through Obscurity“ zu hoffen, ist also keine wirksame Strategie, mit dieser Art von Angriffen umzugehen.

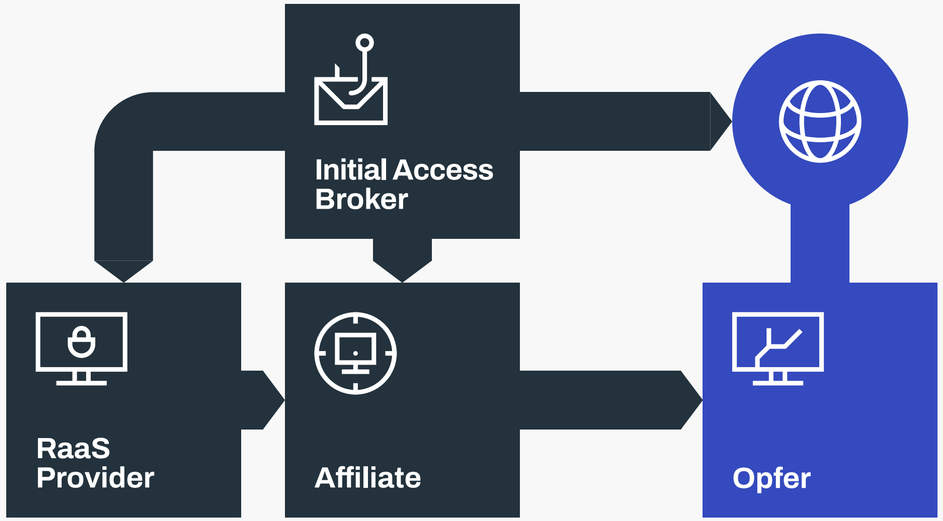
Kriminelle werden nicht nur durch Erpressung reich

Erpressung ist nicht die einzige Einnahmequelle im Cybercrime-Ökosystem. Um die Zahlungsbereitschaft zu erhöhen, behaupten die Bedrohungsakteure mittlerweile häufig, dass sie nicht nur Ransomware eingeschleust, sondern auch Daten ausgeschleust haben. Datenlecks, die bekannt werden, sind peinlich, es drohen teure Geldbußen und der Verlust des guten Rufs, weshalb die Opfer vielfach lieber schweigen und zahlen.

Dieses Modell der doppelten Erpressung ist relativ neu und relativ bekannt. Doch die Angreifer müssen niemanden erpressen, um dennoch satten Gewinn zu erzielen.

Wie? Das Endspiel heißt zwar Erpressung, aber Angreifer verkaufen gerne auch einzelne Komponenten eines Angriffs. Ähnlich wie die gesetzestreue Geschäftswelt sich spezialisiert hat, haben die Bedrohungsakteure im Laufe der Zeit ihre jeweiligen Nischen gefunden und damit das geschaffen, was manchmal als „Cybercrime-Ökosystem“ bezeichnet wird.

Initial Access Brokers – Bedrohungsakteure, die sich mittels Phishing, kompromittierter RDP-Konten oder durch Softwarelücken den ersten Zugang ins Unternehmen verschaffen. Diesen Zugang verkaufen sie dann an andere Akteure, die für die eigentliche Erpressung verantwortlich sind.



RaaS-Provider (Ransomware as a Service) – Plattformen, die diverse Funktionen zur Verfügung stellen, die man für die Erpressung eines Unternehmens braucht, z. B. Malware-Pakete und Angriffstools, Schulungen, Kommunikationskanäle für die Opfer und Geldwäsche-Services mit Kryptowährungen. Ihre Erlöse erzielen sie durch Lizenzgebühren für die Plattformnutzung oder durch die Beteiligung am Lösegeld.

Affiliates (final Ausführende) – Bedrohungsakteure, die das bereits kompromittierte Unternehmen mit Ransomware infizieren, Daten exfiltrieren und die Erpressung im engeren Sinne einleiten. Sie skalieren ihre Bemühungen – und damit ihre Einnahmequellen –, indem sie die Dienste von Initial Access Brokern und RaaS-Anbietern nutzen.

Ökonomie der Diebe

Initial Access Broker werden z. B. von anderen Angreifern für Zugangspakete bezahlt, RaaS-Provider bieten ihre Plattform und ihre Dienste auf der nächsten Stufe (gegen Entgelt) an usw. Dabei ziehen die besten Anbieter mehr Aufträge zu höheren Tarifen an Land, ganz wie in der legalen Welt.

All dies bedeutet, dass Sie in jedem Fall ein Ziel darstellen, auch wenn Sie entschlossen sind, kein Lösegeld zu zahlen, und zuversichtlich sind, dass Sie auf einen Angriff reagieren und sich davon erholen können – einfach deshalb, weil die Cybercrime- Dienstleister immer bezahlt werden, unabhängig davon, ob die Erpressung am Ende gelingt.

Und noch etwas

Diese beiden Faktoren – der offenbare Erfolg von Ransomware-Attacken und die Herausbildung eines Cybercrime-Ökosystems – haben die Schärfe und das Volumen der Angriffe wohl gesteigert, es hat aber noch ein weiterer Faktor zum Siegeszug von Ransomware beigetragen: Zahllose Unternehmen haben ihre Systeme, Anwendungen und Daten für die Cloud geöffnet und ermöglichen Mitarbeitern, Partnern und Kunden den Online-Zugriff von einer Vielzahl von Geräten und Standorten aus. Dadurch hat sich die Anzahl der potenziellen Einstiegspunkte, die geschützt werden müssen, enorm erhöht.

Kurz gesagt: Die Angriffsfläche, die viele Unternehmen nach außen zeigen, hat sich exponentiell vergrößert, während die Angreifer einen Angriff nicht einmal zu Ende bringen müssen, um an ihr Geld zu kommen.

Grund zur Zuversicht

Es gibt immer einen Moment der Wahrheit, in dem es möglich ist, sich zur Wehr zu setzen und siegreich zu bleiben. Aus eigener Erfahrung und aus der Struktur des Cybercrime-Ökosystems wissen wir, dass erpresserische Angriffe einen Lebenszyklus durchmachen, bei dem die Ransomware keineswegs gleich nach dem ersten Zugang eingespielt wird. Die Bedrohungsakteure wollen ihre Chancen auf Zahlung maximieren. Darum kundschaften sie zuerst diejenigen Systeme aus, bei denen Ausfallzeiten wirklich wehtun, und diese infizieren sie dann mit Ransomware. Die Dateien auf dem erstbesten Rechner zu verschlüsseln, auf den sie Zugriff bekommen, würde nicht genügend Druck aufbauen, um das Unternehmen zur Zahlung von Lösegeld zu bewegen.

Die Zeit, die von der Identifizierung eines ersten Zugangs bis zum Einsatz von Ransomware auf geschäftskritischen Systemen bleibt (auch als „time to objective“ bekannt), ist unterschiedlich lang; es können Stunden oder Tage sein. In jedem Fall steht ein Zeitfenster offen, in dem der Angriff entdeckt und entfernt werden kann, **bevor** er sein Ziel erreicht und ernsthafte Auswirkungen auf das Unternehmen hat.

Diesen Moment gibt es fast immer. Die Wahrheit der Wirklichkeit ist aber, dass Unternehmen diese goldene Gelegenheit oft nicht nutzen (können). Der Grund: Ihre Systeme und ihre Incident Response Retainer als Notfallunterstützung sind auf Wiederherstellung ausgelegt und nicht unbedingt auf Reaktion.

Wiederherstellung ist keine Reaktion

Was viele Unternehmen unter „Reaktion“ verstehen, würden wir eher als „Wiederherstellung“ definieren.

Oft wird unser Incident-Response-Team hinzugezogen, nachdem ein Angreifer die Systeme des Unternehmens mit Ransomware verschlüsselt oder anderweitig schwer kompromittiert hat. An diesem Punkt konzentrieren sich die Bemühungen unseres Teams darauf, das Unternehmen wieder online zu bringen, die Geschäftsleitung zu beraten und eine Ex-post-Analyse durchzuführen, um die Ursache zu ermitteln. Dies sind alles notwendige und wichtige Elemente der Wiederherstellung, aber nicht der Reaktion.

Wir wissen, dass unsere Incident-Response-Experten Gold wert sind. Aber sie sind die Ersten, die zugeben, dass es ihnen lieber wäre, wenn sie nicht auf Hilferufe von Unternehmen antworten müssten. Viele der Responder, die zu diesem Report beigetragen haben, sagen, dass sie oft das Gefühl haben, mit Menschen zu sprechen, die gerade die schlimmsten Tage ihrer Karriere erleben. Diesen Menschen zu helfen, dass sich solche Tage nicht immer wiederholen – und täglich grüßt das Murmeltier –, und zwar dadurch, dass sie den richtigen Reaktionsansatz entwickeln, ist etwas, auf das unsere Responder großen Wert legen.

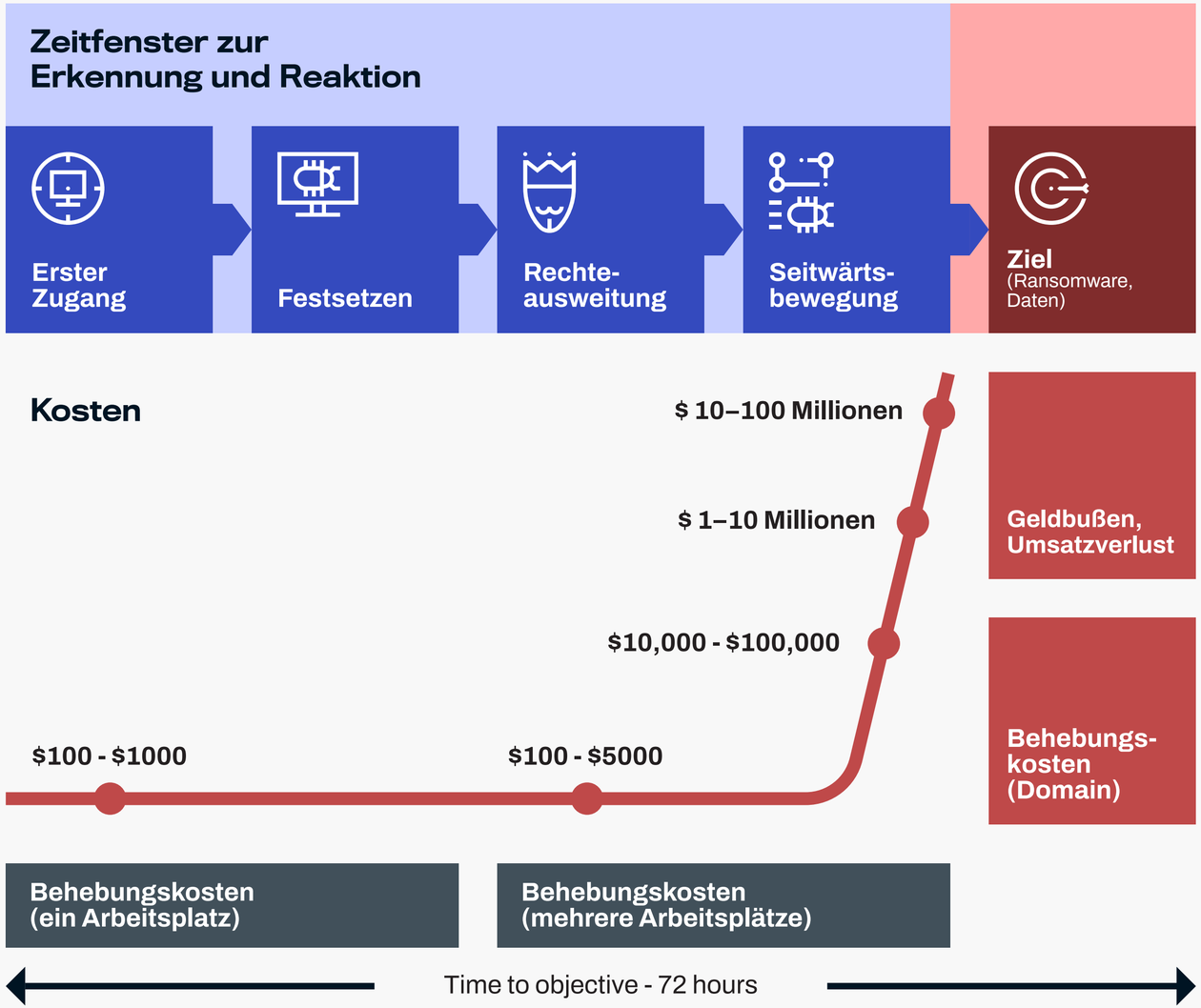
Reaktion kostet weniger als Wiederherstellung

Der Ablauf der derzeitigen Erpressungsangriffe öffnet ein Zeitfenster, in dem der Angriff entdeckt und entfernt werden kann, bevor er ernsthafte Auswirkungen auf das Geschäft hat.

Einen Angreifer zu entfernen, nachdem er sich einen ersten Zugang verschafft hat, aber bevor er ernsthaften Schaden anrichtet, wirft kaum Kosten auf. Eine Stunde, um die Malware zu entfernen, oder ein halber Tag, um ein neues Image aufzuspielen, ist ein Aufwand, der im Vergleich zur Wiederherstellung nach einem ausgewachsenen Vorfall kaum ins Gewicht fällt. Selbst wenn der Angreifer bereits mehrere Rechner kompromittiert hat, beschränken sich die Kosten auf einen Tag Reinigungsarbeit.

Im Gegensatz dazu sind die Kosten, wenn der Angreifer sein Ziel erreicht, deutlich höher. Zum einen ist dann der Behebungsaufwand viel größer (unserer Erfahrung nach dauert es Wochen oder Monate), doch die wirklichen Kosten liegen im Umsatzverlust und in den Bußgeldern. Cognizant schätzt seine Umsatzeinbußen im Folgequartal des Angriffs auf 50 bis 70 Millionen US-Dollar.

Wenn es viel günstiger ist, zu **reagieren, bevor** der Angreifer sein Ziel erreicht hat, als **wiederherzustellen, nachdem** er sein Ziel erreicht hat – warum machen das dann nicht alle?



Warum gibt es die Reaktionslücke?

Bei Unternehmen, die nicht auf einen Angriff reagieren können, bevor er Folgen für das Geschäft hat, liegt eine sogenannte Reaktionslücke vor (diese Response Gap haben wir bereits an anderer Stelle besprochen). Sie kann vielerlei Gründe haben. Die Hauptgründe, von denen die Incident-Response-Teams und die Detection-and-Response-Teams berichten, sind die folgenden:

Ursache	Beispiel
Das Unternehmen hat Erkennungstechnologie, aber niemanden, der die Ergebnisse auf den Schirm bekommt.	Bei einem Opfer schlug das Antivirenprogramm bei Standardmalware zwar an, aber mangels Personal kam die Datei nicht umgehend in Quarantäne, sodass der komplette Serverbestand kompromittiert wurde.
Aufgrund von ungenügender Ausbildung und zu wenig Erfahrung bleibt die Reaktion ineffektiv.	Ein Opfer mit Endpoint Detection and Response reagierte auf kritische Alarme damit, dass es die Rechner sofort vom Netzwerk trennte, woraufhin die Angreifer Ransomware auf hunderte andere Rechner losließen, die nicht als gefährdet identifiziert waren.
Vorhandene Sicherheitskontrollen sind nicht „response-ready“ konfiguriert.	Auf den Gateways eines Opfers war nur das Basis-Logging aktiviert, was die Incident- Response-Ermittlungen erschwerte, sodass die Angreifer länger im Netzwerk blieben.
Mangelnde Budgetplanung verzögert den aktiven Incident-Response-Start.	Ein Kunde brauchte eine Woche, um den Leistungsumfang gegenzuzeichnen – so wurde aus einer normalen Malware-Infektion eine partielle Domain-Kompromittierung.

Schuld an der Lücke ist nicht unbedingt das Unternehmen, sondern oft einfach ein verändertes Umfeld. Die Anpassung an neue Umstände ist jedoch ein notwendiger Schritt. Der Ansatz, den wir vorschlagen, ist etwas, das sich First Response nennt.

First Response ist effektive Reaktion

Wir haben viel darüber gesprochen, dass Reaktion die Beseitigung eines Angreifers ist, bevor er sein Ziel erreicht. Wie funktioniert das in der Realität?

Die Idee hinter First Response ist, die Ursache und das Ausmaß eines Angriffs zu bestimmen, bevor ein Notfallplan zur Eindämmung umgesetzt wird, der den Angreifer aus dem Netzwerk verbannt, ehe sein Treiben geschäftliche Folgen hat.

Das oberste Prinzip von First Response besteht darin, vor allen Gegenmaßnahmen zuerst das Ausmaß des Angriffs zu bestimmen. Eine effektive Eindämmung ist eine, bei der der Angreifer mit einem einzigen Streich eliminiert wird. Das gelingt, wenn Sie wissen, wo sich der Angreifer befindet.

Überstürzt in eine Bekämpfung zu starten, bei der das Ausmaß des Angriffs noch nicht klar ist, kann **unerwartete Konsequenzen** haben. Dazu gehört z. B., dass der Angreifer im Gegenzug Ransomware auf alle Rechner spielt, auf die er noch Zugriff hat, oder dass er wieder in den Tarnmodus wechselt, was ein langwieriges (und kostspieliges) Katz-und-Maus-Spiel zur Folge hat. Solche ungewollten Auswirkungen sind nicht das Reaktionsresultat, das Sie sich wünschen.

An diesem Punkt muss man immer abwägen. Es kann leicht sein, dass man bei einem Angriff voreilige Schlüsse zieht und einen Plan startet, der sich dann als halb gar herausstellt. Automatisierte oder von Playbooks ausgelöste Reaktionen setzen oft auf Schnelligkeit statt auf Effektivität – und das kann Konsequenzen haben, wenn der Angreifer nur teilweise vertrieben wird. Dass eine Reaktionsmethodik eher eine langsame als eine schnelle Reaktion befürwortet, mag manchen merkwürdig vorkommen, aber eine effektive Reaktion braucht eben die Balance von Geschwindigkeit und Präzision, die auf solider Aufklärung beruht.

First Response nutzt das Zeitfenster zwischen der ersten Kompromittierung und der Infizierung mit Ransomware. First Responder kartieren den Weg und das Ausmaß des potenziellen Einbruchs, wobei sie Einzelheiten, Muster und Hinweise wahrnehmen, die von einer automatisierten Reaktion auf das erste Alarmpiepsen unbemerkt bleiben würden. Geschwindigkeit ist das eine, aber zur Bewertung der Geschwindigkeit gehört auch deren Effektivität: Wenn Sie im schnellsten Zug der Welt fahren, werden Sie begeistert sein – bis Sie merken, dass keine Bremsen eingebaut sind.

Die wichtigste Messung nach der First Response sollte prüfen, ob der Vorfall Auswirkungen auf das Geschäft gehabt hat.

Was ist aus Sicht der Praktiker eine gute First Response?

Unsere Incident-Response-Teams und Detection-and-Response-Teams haben fünf Hauptmerkmale einer effektiven Erstreaktion (First Response) identifiziert:

1 Sichtbarkeit

Die Möglichkeit, verlässliche Rückschlüsse darauf zu ziehen, wie ein Angreifer Zugang zum Netzwerk erlangt und es kompromittiert hat, ist entscheidend für die Entwicklung und Ausführung eines halbwegs sicheren Abhilfeplans. Sichtbarkeit beginnt mit einem Endpoint- Detection-and-Response-Agenten, der eine große Bandbreite an Daten und forensischen Artefakten erfasst.

2 Wissen über den Angreifer

Erfahrung und Wissen um den Modus Operandi eines Angreifers tragen zu einem effektiven Abhilfeplan bei. Wenn Sie z. B. die typischen Arbeitszeiten des Angreifers kennen, können Sie das optimale Zeitfenster bestimmen, in dem Sie die Abhilfe-maßnahmen durchführen.

3 Stakeholder Management

Angriffssituationen sind enorm stressig und unangenehm, vor allem wenn man so etwas zum ersten Mal erlebt. Es ist wichtig, die Betroffenen ruhig zu halten, indem man ihnen den Prozess im Vorfeld erklärt, sie auf dem Laufenden hält und bei Bedenken zur Verfügung steht.

4 Integrierte Tools

Wer Erkennungs-, Untersuchungs- und Reaktionsfunktionen in einem einzigen Tool verfügbar macht, hält Verzögerungen und menschliche Fehler minimal – das kann den Unterschied zwischen einem erfolgreichen und einem gescheiterten Abhilfeplan ausmachen.

5 Menschliche Beteiligung

Es ist wichtig, dass Menschen vor Ort sind, um Kontext, Erfahrung und Einfühlungsvermögen einzubringen. Tools und Automatisierung können kontraproduktiv wirken, wenn sie nicht von menschlicher Erfahrung und Intuition gestützt werden.

First Response in Aktion

Um zu veranschaulichen, was wir unter First Response verstehen, wollen wir von zwei Vorfällen berichten, die die Effektivität dieser Methodik demonstrieren.

Fallstudie

1: Eine wohldurchdachte Reaktion bei der Inbetriebnahme

Unser Team begann gerade, den MDR-Service (Managed Detection and Response) von WithSecure™ bei einem großen Anlagenbauer aus der Energiebranche einzurichten. Unsere Experten entdeckten sofort Cobalt Strike im Netzwerk, ein weit verbreitetes Angreifer-Framework. Bei genauerer Untersuchung wurden elf infizierte Komponenten gefunden, darunter sechs Domain-Controller.
Die verwendeten Angriffstechniken stimmten mit denen einer Ransomware-Bande überein, mit der wir zuvor schon zu tun gehabt hatten, was dem Team einen guten Hinweis darauf gab, was der Angreifer als Nächstes vorhatte und wann. Da wir in diesem Fall mit hoher Wahrscheinlichkeit davon ausgehen konnten, dass der Angreifer seine Ransomware im Laufe des Wochenendes in großem Stil platzieren würde, hatte unser Team eine ziemlich genaue Vorstellung davon, wie viel Zeit ihm und dem Kunden blieb, um eine adäquate Reaktion zu entwickeln.

Wäre die Bedrohung unentdeckt geblieben oder hätte das Unternehmen versucht, die Hacker hinauszuwerfen, bevor das Ausmaß des Schadens klar war, hätte der Angriff die Produktion des Unternehmens für einen längeren Zeitraum zum Stillstand bringen und das Unternehmen wirtschaftlich lähmen können.

In enger Zusammenarbeit mit dem Sicherheitsteam des Kunden waren wir in der Lage, einen Abhilfeplan zu entwickeln, der schnell und effektiv umgesetzt werden konnte, und zwar ohne das Risiko, die Hacker zu warnen. Gemeinsam beendeten wir die Schadprozesse, während der Kunde den Zugang über die Firewall blockierte und die Domain-Anmeldedaten zurücksetzte. So konnten wir den Angreifer mit einer einzigen Gegenoffensive entfernen und seine Rückkehr verhindern.

Wichtige Punkte:

1. Wir waren in der Lage, rasch einen Abhilfeplan zu entwickeln und auszuführen, obwohl wir eigentlich im Nachteil waren: Wir hatten den Angriff erst in seinem fortgeschrittenen Stadium entdeckt, als wir bei dem neuen Kunden unseren Agenten einrichteten. Möglich war diese Reaktion, weil wir zuvor schon mit dem Angreifer zu tun gehabt hatten und wussten, wie er arbeitet.
2. Die Kosten für das Unternehmen wurden erheblich reduziert, weil MDR mit First Response gerade noch rechtzeitig zum Einsatz kam, um den Angriff abzufangen, bevor er ernsthafte Folgen für das Geschäft haben konnte.

2: Klassische Entdeckung und Wiederherstellung contra First Response

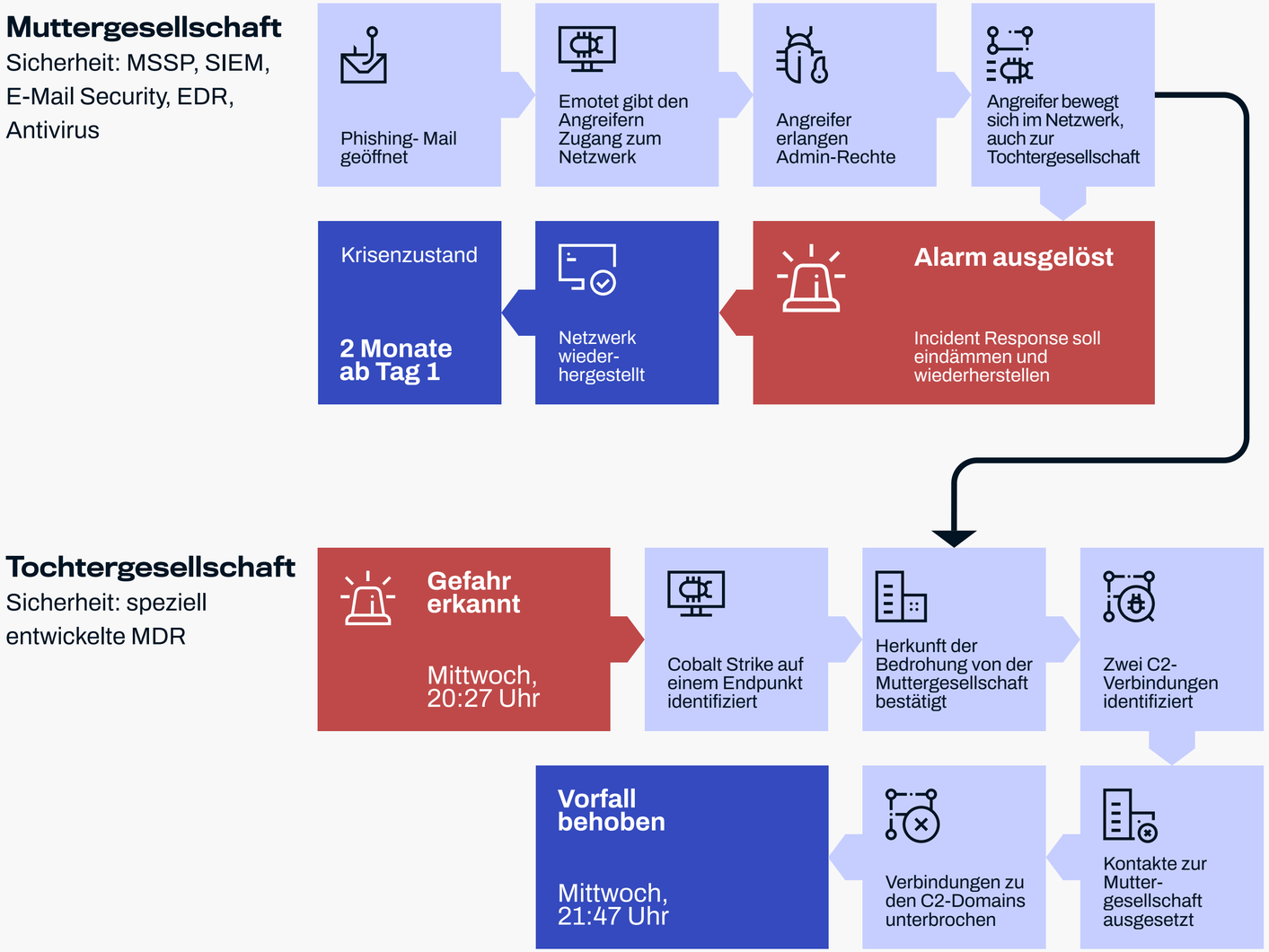
Die folgende Geschichte ist vielleicht das beste Beispiel dafür, warum die richtige Reaktion so entscheidend ist. Es geht darin um ein großes Unternehmen ohne effektive Reaktion und um eine seiner Tochtergesellschaften, die ein Countercept-Kunde von WithSecure™ ist.

Die Muttergesellschaft nutzte die E5-Suite von Microsoft, beschäftigte einen regionalen Managed Security Service Provider und hatte einen Incident Response Service eines großen Beratungsunternehmens beauftragt. Angreifern gelang es aber, die Verteidigung des Unternehmens zu umgehen und sich, sobald sie im Netzwerk waren, erweiterte Rechte zu verschaffen. Dieser Zugang ermöglichte es ihnen auch, in die Systeme der Tochtergesellschaft einzudringen – in die unseres Kunden.

Die Muttergesellschaft rief ihren Incident Response Provider, der mit Dutzenden von Beratern anrückte und das Unternehmen über einen längeren Zeitraum eine sechsstellige Summe kostete. Dem Unternehmen wurde gesagt, dass es einem fortschrittlichen Angriff zum Opfer gefallen sei, möglicherweise durch einen nationalstaatlichen Akteur.

Übermäßiges Vertrauen auf technische Reaktionen sieht vielleicht auf dem Papier gut aus, doch sie können sich in der Praxis als gefährlich schwach erweisen, wenn sie nicht mit dynamischem Input von erfahrenen Reaktionsteams kombiniert werden.

Fallstudie



Eine Phishing-Mail ist nie „Game Over“

Als wir unsere eigene Ex-post-Analyse durchführten, stellten wir fest, dass der Angriff keineswegs auf einen fortschrittlichen nationalstaatlichen Akteur, sondern auf eine opportunistische Ransomware-Bande zurückging. Ein User des Mutterunternehmens hatte eine Phishing-Mail geöffnet und damit Emotet heruntergeladen, einen gewöhnlichen, zum Botnet ausgebauten Banking-Trojaner, der dazu dient, erste Zugänge zu legen, die verkauft werden können. Der Trojaner ist so weit verbreitet, dass er hätte erkannt und entfernt werden müssen, lange bevor er die höhere Rechteposition erlangte, die dann dazu genutzt wurde, die Tochtergesellschaft zu infiltrieren.

Sieht man sich die Kosten für das Unternehmen und die Betriebsunterbrechung an, könnte der Kontrast zwischen den beiden Reaktionsstrategien kaum größer sein: Die eine schlug allein bei den Wiederherstellungskosten mit einem sechsstelligen Betrag zu Buche, die andere wurde im Rahmen der von der Grundgebühr gedeckten Leistungen behoben, bei so gut wie gar keiner Unterbrechung des Geschäftsbetriebs.

Fazit

Response-Teams und Technologie so nah wie möglich an den Ort der Entdeckung zu ziehen, ist nicht mehr nur wünschenswert, sondern Pflicht.

Erkennung und Reaktion müssen zeitnah erfolgen. Insofern ist es verständlich, dass viele Security-Anbieter gern davon reden, wie schnell Reaktionen sind, die automatisiert oder auf Knopfdruck erfolgen. Wir glauben nicht, dass dies ein guter Ansatz ist. Es müssen Menschen beteiligt sein. Und es ist von entscheidender Bedeutung, dass das Team, das die Erstreaktion übernimmt, sich eng mit dem Incident-Response-Team abstimmt. Außerdem muss die Reaktion umfassend sein, anstatt automatisiert und unvollständig.

Mitten in der Reaktion auf einen potenziellen Vorfall ist es freilich schwer, einen kühlen Kopf zu bewahren. Dennoch müssen die geschäftlichen Auswirkungen nach der Reaktion das Maß des Erfolgs sein – und nicht wie schnell der erste Schuss abgefeuert wird. Reflexartige Reaktionen richten am Ende oft mehr Schaden an als eine überlegte, geplante, umfassende und gründliche Vertreibung des Eindringlings.

Eine gute First Response erfordert eine Kombination aus menschlichem Fachwissen und speziell entwickelten, integrierten Tools, die nah an den Einstiegspunkten einer Kompromittierung platziert sind. Dann können die First Responder sich schnell ein Bild davon machen, was während des Vorfalls passiert, und potenzielle Kompromittierungen ausschalten.

Wenn ein Anbieter Erkennung und Reaktion aus einer Hand leistet, so kann das für den Kunden wirklich effektiv sein. Damit wird dem Unternehmen allerdings ein ziemlich großer Vertrauensvorschuss abverlangt, der für manche noch ungewohnt ist. Der Anbieter muss an den bestehenden Prozessen ausgerichtet werden, Zugang und Verantwortung können nicht einfach en bloc übergeben werden – dieses Maß an Vertrauen muss man sich erst verdienen.

Starke MDR-Services, die dabei helfen, Angriffe zu identifizieren, zu erkennen und auf sie zu reagieren, bevor sie zu Vorfällen werden, machen für viele Unternehmen einen gewaltigen Unterschied: Dank der Fähigkeiten, die Detection-and-Response- Teams mitbringen, insbesondere in Verbindung mit dedizierten Tools und Support, können Unternehmen vermeiden, dass sich ein Drama zur Krise auswächst.

Wenn Sie mehr darüber erfahren wollen, wie First Response Ihr Risiko und die Auswirkungen auf Ihr Unternehmen reduzieren kann, dann sprechen Sie am bestem mit jemandem aus den MDR-Teams von WithSecure™.
dach-mdr@withsecure.com

Über WithSecure™

WithSecure™ ist Ihr zuverlässiger Partner für Cybersicherheit. IT-Dienstleister, MSSPs und Unternehmen sowie die größten Finanzinstitute, Hersteller und Tausende der weltweit avanciertesten Kommunikations- und Technologieanbieter vertrauen uns bei ergebnisorientierter Cybersicherheit, die ihren Betrieb schützt und verbessert. Unser KI-gesteuerter Schutz sichert Endgeräte und Cloud-Zusammenarbeit, und unsere intelligenten Detection-and-Responsefunktionen werden von Spezialisten bereitgestellt, die Geschäftsrisiken aufdecken, indem sie proaktiv nach Bedrohungen suchen und Angriffe in Echtzeit abwehren. Unsere Berater arbeiten mit Unternehmen und Technologieanbietern zusammen, um durch faktenbasierte Sicherheitsberatung Resilienz zu gewährleisten. Mit über 30 Jahren Erfahrung in der Entwicklung von Technologien, die den Unternehmenszielen entgegenkommen, haben wir unser Portfolio so entwickelt, dass wir mit unseren Partnern durch flexible Geschäftsmodelle weiter wachsen können.

WithSecure™ (ehemals F-Secure for Business) wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd. notiert.

WITH secure™