Broschüre

Einsatz- und reaktionsbereit bei Zwischenfällen

Vorbereiten, untersuchen, reagieren, wiederherstellen – und dann verbessern

WITH secure

Inhalt

Warum Incident Response?

Incident Response (IR), die rasche Reaktion auf Zwischenfälle, ist heute anspruchsvoller denn je. Cloud-Services erschweren die IT-Sicherheit, es fehlt an Know-how, und die Verantwortung wird mit Cloud-Service-Providern (CSPs) geteilt. Wenn Fehler passieren und es zu einem Zwischenfall kommt, kann die Kooperation des CSPs begrenzt sein.
Es steht viel auf dem Spiel: Ein professionell bearbeiteter Zwischenfall kann binnen einiger Stunden bereinigt sein – statt nach Tagen oder Monaten; IR- und Rechtskosten in Millionenhöhe lassen sich vermeiden; Vorstände, die eine solche Krise erfolgreich gemeistert haben, können ihre Karriere fördern.

Alarmierende Zahlen

- Bis zu 4.000 Beschwerden über Cyberangriffe täglich registrierte die Cyberabteilung des FBI im Jahr 2020. Und die durchschnittlichen Kosten einer Datenpanne betrugen laut einem Bericht von IBM und dem Ponemon Institute im selben Jahr 3,86 Millionen Dollar.

- Laut Data Breach Incident Report (DBIR) von 2021 waren rund 15 % der 29.000 analysierten Sicherheitszwischenfälle mit Ransomware verbunden, weltweit insgesamt 32.000 Sicherheitsverletzungen aller Art pro Tag.

- Nach Angaben der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) sind weltweit 41.000 von insgesamt 213 Millionen Unternehmen börsennotiert. Das heißt, selbst wenn sich Cyberangriffe nur auf börsennotierte Unternehmen konzentrieren würden, würde ein börsennotiertes Unternehmen im Durchschnitt weniger als einen Zwischenfall pro Jahr erleben.

Allerdings: Große Organisationen haben zwar ihre eigenen IR-Teams, aber diese sind einfach nicht mit einem Umfang und einer Vielfalt von Zwischenfällen konfrontiert, die zur Entwicklung und Gewährleistung wirklicher Abwehrkapazitäten erforderlich wäre. Deshalb: Wenn Sie nur einen einzigen Sicherheitsservice auslagern wollen, dann unbedingt IR.

Unsere Unterstützung

- **Under Attack:** für Organisationen, die jederzeit anrufen können und denen wir mit allen verfügbaren Ressourcen helfen
- **Incident Response Retainer:** garantierte Reaktion bei Cyberangriffen
- **Incident Readiness:** trainieren und verbessern Sie Ihre Reaktionsfähigkeit bei Zwischenfällen ohne Unterbrechung Ihres Geschäftsbetriebes

Wir arbeiten für Dow Jones-, NASDAQ- und FTSE 100-Unternehmen sowie für Regierungsbehörden und Ministerien weltweit. Der Kampf gegen neuartige, anhaltende Bedrohungen (Advanced Persistent Threats, APTs) und Crimeware-Akteure ist unser tägliches Geschäft.

Unsere Leistungen

In den 12 Monaten bis August 2021 führte unser blaues Team 1.226 Überprüfungen durch, von denen 103 den Einsatz des IR-Teams in direkter Zusammenarbeit mit den Teams der Kunden erforderten. Das waren jeden Tag im Schnitt mehr als drei Untersuchungen. Ein solches Maß an wirklicher Praxiserfahrung und Teamwork ist in einer einzelnen Organisation nicht zu erreichen.

Countercept Host Agent

Der Countercept-Agent für Endgeräte ist unser leistungsstärkstes Tool für die Instant Response. Er sammelt die für die Untersuchung von Zwischenfällen erforderlichen Telemetriedaten und spart Zeit und Reisekosten durch die Fernabfrage von Objekten, die Isolierung von Hosts, das Beenden verdächtiger Prozesse, das Entfernen von Persistenzmechanismen und das Löschen von Schaddateien.

- **Zugang zu hochqualifiziertem Fachwissen und Technologie für die Reaktion auf Zwischenfälle:** Unsere Senior Consultants bearbeiten jährlich über 30 Zwischenfälle. Wir entwickeln und vertreiben Threat-Hunting-Tools wie Chainsaw, um Geschwindigkeit und Qualität der Prüfungen zu erhöhen.
- **Sicherstellung Ihrer Fähigkeit zum Krisenmanagement:** Wir sind technologieunabhängig und arbeiten mit den verfügbaren Technologien, um Ihren Auftrag zu erfüllen. Wir betreiben auch einen eigenen Host-Agenten, um flexibel auf Ihren Zwischenfall reagieren zu können – mit einer auf den jeweiligen Angriff angepassten Erkennung.
- **Stärkung durch Co-Security:** Wir helfen Ihnen beim Aufbau eines zuverlässigen Teams für die Incident Response in der Cybersicherheit (CSIRT), das so geschult und ausgerüstet ist, dass es auch unter Druck unter verschiedensten Bedingungen reagieren kann.
- **Betriebliche Resilienz:** Durch gemeinsame Entwicklung und Prüfung Ihrer Richtlinien, Verfahren, Rollen und Technologien für die Incident Response minimieren wir die geschäftlichen Auswirkungen einer Cyber-Sicherheitskrise und bereiten Sie auf die Anpassung, das Lernen und die Wiederherstellung nach Angriffen vor.

Under Attack

Als Gründungsmitglied des Certified IR Scheme am britischen National Cyber Security Centre verfügen wir über breite Erfahrung in der Reaktion auf Zwischenfälle mit nationaler Tragweite. Wir reagieren auf Zwischenfälle bei Angriffen auf komplexe Unternehmensnetzwerke und entwickeln Playbooks sowie Tools, um unsere Reaktionsfähigkeit bei Cloud-Service-Zwischenfällen zu stärken.

Under Attack ist unser einfachstes und flexibelstes Geschäftsmodell, das auf Zeit- und Materialaufwand für die Reaktion bei Zwischenfällen basiert.

Incident Response Retainer

Unser IR-Retainer bietet Unternehmen Zugang zu den Qualifikationen der besten IR-Spezialisten mit vereinbartem SLA, um auch bei branchenweiten Ereignissen den nötigen Support zu sichern, wenn solche Spezialisten anderweitig stark gesucht sind (wie bei Microsoft Exchange, SolarWinds oder Log4j 2).

Unser Onboarding-Prozess umfasst die Überprüfung der Betriebsverfahren und der IT-Umgebung des Kunden im Rahmen mehrerer Workshops mit den wichtigsten Beteiligten, den Mitgliedern des Incident-Response-Teams und den bestellten First Respondern.

Die erste Einschätzung erfolgt binnen drei Stunden (aktueller Durchschnitt: ca. 15 Minuten) nach Bestellung des Services über eine von erfahrenen First Respondern besetzte Hotline, gefolgt von einer Remote-Unterstützung durch einen Prüfer innerhalb von drei Stunden und bei Bedarf einer Unterstützung vor Ort.

Wir kommen regelmäßig mit unseren Kunden zusammen und informieren sie über die Ergebnisse unserer Untersuchungen von Zwischenfällen, unseres Threat Huntings sowie über relevante, aktuelle Angreifer und deren Methoden. Wir bieten verwaltete Dienste an, um Kunden bei der Verteidigung gegen effektiv getarnte Angriffe zu unterstützen. Mit unserem Know-how in offensiver Sicherheit entwickeln wir neue Wege, um unsere Kunden proaktiv zu schützen. Und wir reagieren auf Angriffe mit dem nötigen Geschick, um Auswirkungen auf das Geschäft zu minimieren.

Das Geschäftsmodell

Wir bieten einen Jahresvertrag an, bei dem der Kunde im Voraus für eine bestimmte Anzahl von Ermittlungstagen bezahlt, mit der Garantie, dass binnen 3 Stunden nach einem gemeldeten Zwischenfall unser Service zur Verfügung steht. Dieses Modell bietet zwei große Vorteile:

- garantierte rasche Hilfe im Bedarfsfall
- stärkere betriebliche Widerstandsfähigkeit durch vorbereitende Maßnahmen, mit denen wir Zwischenfälle schneller eindämmen und so die Gefahr von Datenverlusten und Unterbrechungen wichtiger Unternehmensdienste verringern.

Modell	Hotline	Garantierter Response	Strategische Entwicklung	Vorausbezahlte Bereitschaftstage	Vorausbezahlte Prüfungs und Reaktionstage	Preisnachlässe
Core	Rund um die Uhr Zugang zur WithSecure-Response-Hotline mit Remote-Support und Beratung von geschulten First Respondern	Remote-Reaktion binnen 3 Stunden (aktuell ca. 15 Minuten)	Umfassendes Onboarding und viertel- oder halbjährliche Service-Reviews mit Diskussion von Bedrohungsdaten und einschlägigen Untersuchungen	nicht angeboten	10 Tage jährlich stets inklusive	10 % Nachlass auf alle weiteren Untersuchungstage
Plus	wie oben	wie oben	wie oben	Mindestens 10 Tage jährlich	10 Tage jährlich stets inklusive	20 % Nachlass auf alle weiteren Untersuchungstage

Incident Readiness

Unternehmen, die bereits über solide Grundlagen in Bezug auf die Reaktionsfähigkeit verfügen, können eine reaktive Incident Response vermeiden, Kostensenkungen erzielen, die Ausgaben kalkulieren und ihre abteilungsübergreifende Kooperation stärken. Partnerschaft und Zusammenarbeit sind hier besonders gefordert, ob bei der Leitung von Einsätzen oder bei der Ergänzung Ihrer Teams in Stoßzeiten und bei langwierigen Zwischenfällen.

Unsere Readiness-Aktivitäten dienen dazu, Ihre grundlegende Reaktionsfähigkeit zu konsolidieren, bevor wir darauf aufbauen: Wir verbessern Qualität und Leistung von Playbooks, üben die Reaktion auf einen realen Zwischenfall in Simulationen und schulen Sicherheitsteams in der korrekten Konfiguration von Tools.

Wie sich der Service weiterentwickeln wird

Unser Ziel ist es, den Engpass an qualifizierten Ressourcen für die Incident Response aufzubrechen und unseren Kunden noch bessere Leistungen zu bieten. Dazu führen wir ein klares, kalkulierbares und ergebnisorientiertes Geschäftsmodell ein.

Unsere Kunden erhalten auf Wunsch standardisierte Pakete mit bestimmten Leistungen für die Incident Response, z. B. Scannen von Endgeräten, Malware-Analyse, Sammeln von Beweisdaten, außerdem Zeit- und Materialpreise, um neue oder spezifische Anforderungen zu erfüllen. Die ergebnisabhängige Preisgestaltung verbessert die Kalkulierbarkeit und gewährleistet Flexibilität.

Im Zuge dieser Entwicklung investieren wir weiterhin in die Verbesserung von Tools und die Automatisierung von Aufgaben bei der Incident Response, um Zeiteffizienz, Geschwindigkeit und Skalierbarkeit zu erhöhen sowie die Kommunikation und den Informationsaustausch zu verbessern und so Angriffe effektiver einzudämmen und abzustellen.

Unsere Methodik

Unsere Methodik basiert auf dem branchenüblichen NIST-Lebenszyklus für die Incident Response und wurde im Zuge zahlreicher Zwischenfälle mit hochentwickelten, permanenten Bedrohungen verfeinert:

Stufe 1: Vorbereitung - Wir helfen Ihnen, Ihre Resilienz gegen Angriffe durch Readiness- und Retainer-Services aufzubauen.

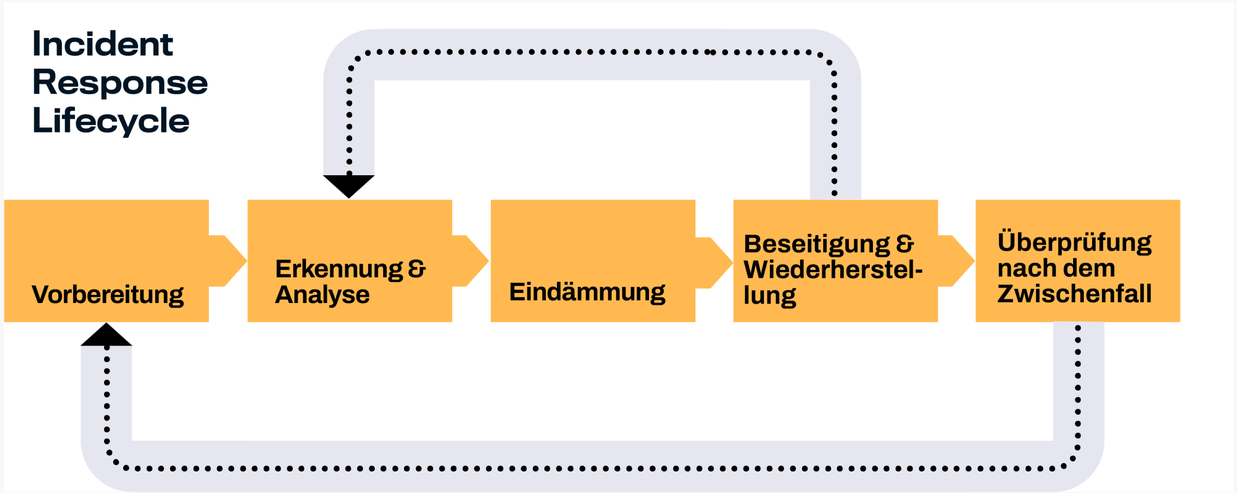
Stufe 2: Erkennung und Analyse - Wenn Sie uns kontaktieren, klären wir hierzu rasch Umfang und Ziele. Bei Bedarf setzen wir unseren Countercept-Agenten im gesamten Unternehmen ein, um Informationen zu sammeln, infizierte Systeme und Persistenzmechanismen zu identifizieren und zu eruieren, womit der Angreifer remote auf das Netzwerk zugreift – mit dem Ziel, unentdeckt so viel wie möglich herauszufinden.

Stufe 3: Eindämmung - Gemeinsam mit Ihrem IT-Team planen wir eine Eindämmungsstrategie, um die Möglichkeiten des Angreifers zu begrenzen, zurückzuschlagen und plötzliche, weitreichende Schäden zu bewirken.

Stufe 4: Beseitigung - Ist der Angriff eingedämmt und liegen die nötigen Informationen über das Verhalten des Angreifers vor, stimmen wir uns mit Ihrem IT-Team ab, um den Angreifer zu stoppen. Der Countercept-Agent entfernt hartnäckige Malware remote.

Stufe 5: Zyklische Wiederholung - Meist versuchen Angreifer, sich erneut Zugang zur Umgebung zu verschaffen. Wir wiederholen den Zyklus zwischen Erkennung und Beseitigung, bis die Bedrohung sicher beseitigt ist. Mit dem Agenten treffen wir Sofortmaßnahmen gegen alle erneuten Versuche, das Netzwerk zu infiltrieren. Zugleich analysieren wir die forensischen Daten, um eventuell noch unbekannte Ursachen für den Zwischenfall zu finden.

Stufe 6: Überprüfung nach dem Zwischenfall - Sie erhalten von uns binnen 5 Tagen nach dem Zwischenfall einen Bericht. Wenn möglich, nutzen wir Bedrohungsdaten, um die Bedrohung zuzuordnen. Wir können außerdem in einer Folgesitzung mit der Führungsebene Empfehlungen zur Risikominderung für weitere Angriffe aussprechen. Auf Wunsch verlängern wir den Zeitraum der aktiven Überwachung und unterstützen Sie durch unseren erweiterten Beratungsdienst.



Wer wir sind

Ein hohes Sicherheitsniveau erfordert Partnerschaft. Wir bieten genau die Partnerschaft, die Unternehmen brauchen, um sich gegen Cybersicherheitsbedrohungen zu wehren. Mit unserer Erfahrung und unseren Kompetenzen, entwickelt in über 30 Jahren, schützen wir weltweit die wichtigsten Unternehmen. Wir können mit Stolz sagen, dass keiner unserer Kunden einen nennenswerten Verlust erlitten hat, während wir ihn geschützt haben. Deshalb bestehen so viele unserer Partnerschaften seit zehn Jahren oder länger.

- Wir sind einer von nur 9 NCSC-zertifizierten Anbietern für Incident Response.
- Unser Spezialgebiet ist die Unterstützung unserer Kunden beim Erreichen operativer Resilienz durch Eindämmung aktueller Angriffe bei gleichzeitiger Fortführung des normalen Geschäftsbetriebs.
- Wir sind toolunabhängig, greifen aber bei Bedarf auf unsere eigene, weltweit führende EDR-Lösung für unsere Kunden zurück.
- Wir sind forschungsorientiert, entwickeln uns gemeinsam mit unseren Kunden ständig weiter und haben neue Tools und Techniken speziell für den Umgang mit Cloud-Angriffen entwickelt.

Über WithSecure™

WithSecure™, ehemals F-Secure Business, ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, Managed Security Services Provider und andere Unternehmen vertrauen WithSecure™ – wie auch große Finanzinstitute, Industrieunternehmen und führende Kommunikations- und Technologieanbieter. Mit seinem ergebnisorientierten Ansatz der Cybersicherheit hilft der finnische Sicherheitsanbieter Unternehmen dabei, die Sicherheit in Relation zu den Betriebsabläufen zu setzen und Prozesse zu sichern sowie Betriebsunterbrechungen vorzubeugen. WithSecure™ nennt diesen Ansatz „Outcome-based Cyber Security“. KI-gesteuerte Sicherheitsmaßnahmen sichern Endpoints und die Zusammenarbeit in der Cloud mit intelligenten Erkennungs- und Reaktionsmechanismen. Die Detection & Response-Experten von WithSecure™ identifizieren Geschäftsrisiken, indem sie proaktiv nach Bedrohungen suchen und bereits laufende Angriffe abwehren – dabei arbeiten sie eng mit Instituten, großen Unternehmen und innovativen Tech-Firmen zusammen. Sie haben mehr als 30 Jahre Erfahrung in der Entwicklung von Technologien, die sich an den Bedürfnissen der Unternehmen orientieren. Das Portfolio von WithSecure™ eröffnet durch flexible Vertriebsmodelle die Möglichkeit, gemeinsam mit Partnern zu wachsen.

WithSecure™ Corporation wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd. gelistet.

WITH secure