RAPID7

Vorbereitung für den Angriff: Entwicklung eines Incident Response Plan

ERIC SUN, SENIOR SOLUTIONS MANAGER, DETECTION & RESPONSE
JEREMIAH DEWEY, DIRECTOR OF INCIDENT RESPONSE

INHALTS-VERZEICHNIS

EINLEITUNG

Im Angesicht zunehmender Cyberangriffe und einer sich rasant entwickelnden IT, müssen Organisationen, die mit vertraulichen Daten arbeiten, Sicherheitsverletzungen erkennen und umgehend beheben können. Externe Spezialisten können helfen, doch diese erst in akuten Krisensituationen einzuschalten, ist äußerst riskant.

Stattdessen sollten IT-Organisationen und ihre Partner die Voraussetzungen für eine möglichst effektive und effiziente Bekämpfung von Sicherheitsverletzungen schaffen. Das Entwickeln und Testen eines Incident Response Plan (IRP, Vorfallreaktionsplan) steht dabei an erster Stelle.

Ein gut durchdachter IRP kann Ihre Organisation auf das Schlimmste vorbereiten und dabei die beste Leistung herausholen. Im Falle einer schwerwiegenden Sicherheitsverletzung dient der Incident Response Plan in jedem Schritt als Blaupause.

Dieses vierteilige E-Book enthält detaillierte Informationen zum Entwickeln und Testen eines IRP. Zudem stellen wir Erkenntnisse vor, die wir in Tausenden von Incident-Response-Einsätzen gewonnen haben.

IM FALLE EINER SCHWERWIEGENDEN SICHERHEITSVERLETZUNG DIENT DER INCIDENT RESPONSE PLAN IN JEDEM SCHRITT ALS BLAUPAUSE.

SCHRITT 1: PLAN ENTWERFEN

In diesem Kapitel werden die Komponenten vorgestellt, die einen effektiven Incident Response Plan ausmachen. Diese reichen von der Definition von Rollen und der Erstellung von Kontaktdaten über die Identifizierung gefährdeter Assets bis hin zum Entwurf von Notfallplänen.

Zusammentrommeln der Truppen

Da im Falle einer Verletzung der Computer- und Netzsicherheit die gesamte Organisation betroffen sein kann, müssen alle Bereiche in die Entwicklung des Plans einbezogen werden. Neben den üblichen Verdächtigen aus IT und Sicherheit gehören dazu auch die PR- und Rechtsabteilungen sowie das leitende Führungsteam.

Doch damit nicht genug: Involvieren Sie auch Lieferanten wie Internetanbieter, externe IT-Firmen und Berater, die im Falle einer Verletzungen der Computer- und Netzsicherheit betroffen sein könnten. Es bietet sich an, zu diesem Zeitpunkt die Kontaktdaten und vertraglichen Vereinbarungen mit Ihren Lieferanten zu prüfen.

KONTAKTLISTE ERSTELLEN

www.rapid7.com/IR-templates

Schließlich wollen Sie nicht erst im akuten Notfall feststellen, dass Ihre SLAs keine zügige Reaktion ermöglichen.

Außerdem sollte jeder Stakeholder im Team seine Rolle bei der Abwehr von Sicherheitsverletzungen verstehen. Wir haben einen Kontaktbogen mit kurzen Beschreibungen möglicher Teamrollen und eine Vorlage für Notfallkontakte für Sie zusammengestellt (zu finden über den Link auf der vorherigen Seite sowie im Anhang dieses E-Books).

Auskundschaften der Umgebung

Im nächsten Schritt sollten Sie herausfinden, welche Assets im Falle einer Sicherheitsverletzung gefährdet wären. Skizzieren Sie Ihre Netzwerkinfrastruktur einschließlich aller Verbindungen zu anderen Organisationen. Dadurch kann Ihr Team den Ausgangszustand des Netzwerks überblicken und Schwachstellen identifizieren.

Fast alle Cyberangriffe werden aufgrund von Schwachstellen in drei Kategorien ermöglicht: **Sicherheitslücken, Fehlkonfigurationen und schwache oder gestohlene Zugangsdaten**. Durch die Identifizierung von Schwachstellen in diesen Kategorien können Bereiche mit Verbesserungspotenzial herausgestellt und beispielsweise mit strengerer Netzwerksegmentierung oder privilegierter Zugangsverwaltung gegengesteuert werden. Ein Defense-in-Depth-Konzept erschwert Eindringlingen den Zugriff auf vertrauliche Ressourcen und bietet Ihrem Team zusätzliche Erkennungs- und Abwehrmöglichkeiten.

Neben unternehmenseigenen Assets sollten auch fremdgesteuerte und externe Assets, wie mobile Mitarbeiter und Cloud-Services, berücksichtigt werden.

Skizzieren Sie anschließend Ihre Präventions- und Erkennungsfähigkeiten einschließlich aller Erkenntnisse aus vergangenen Penetrationstests. Bonuspunkte gibt es, wenn Ihre Organisation bereits Angriffe simuliert und über interne Red-Team-Ressourcen verfügt.

Anschaulich dargestellte Konsequenzen eines erfolgreichen simulierten Angriffs überzeugen die Führungsebene wahrscheinlich eher als technische Details zur Priorisierung von Schwachstellen. Das alles kann Ihnen dabei helfen, die benötigten Ressourcen zum Entwickeln und Testen Ihres Plans in einem Business Case darzulegen.

Dokumentieren der Schwachstellen

Nachdem nun alle zu schützenden Assets bekannt sind, steht die Organisation vor der Aufgabe, potenzielle und tatsächliche Gefährdungen zu identifizieren. Ein klar definierter, wiederholbarer Untersuchungsworkflow kann Ihrem Team dabei helfen, die Ausmaße eines Störfalls zu bestimmen und schnell die richtigen Stakeholder einzubeziehen.

Dazu werden zunächst diejenigen Assets erfasst, die nur eingeschränkt isoliert und korrigiert werden können. Dazu zählen beispielsweise Privatgeräte und Assets externer Lieferanten, die nicht durch Ihre Sicherheitsinfrastruktur abgedeckt sind.

Setzen Sie anschließend die berüchtigte schwarze Kapuze auf und versuchen Sie, wie ein Hacker zu denken. Wo liegen die aussichtsreichsten Angriffsziele? Welche Assets und Benutzer haben Zugriff auf diese Ziele, und welche Folgen hat eine Kompromittierung kritischer Zugangsdaten? Sind diese Informationen schon im Vorfeld bekannt, können die Ausmaße eines Angriffs später besser nachvollzogen werden.

Rüsten für den Notfall

Welche Optionen stehen zur Aufrechterhaltung des Geschäftsbetriebs zur Verfügung, wenn wichtige Assets ausfallen oder abgeschaltet werden müssen?

Failover- und Back-up-Strategien helfen Ihrem Team, auf die Kompromittierung von Daten und Systemen zu reagieren. An dieser Stelle wird es sich auszahlen, neben der IT auch andere Stakeholder einbezogen zu haben.

SCHRITT 2: PLAN ÜBERPRÜFEN

Im letzten Entwurfsschritt des Incident Response Plan sollten die Kommunikationsabteilungen Ihrer Organisation Vorlagen erstellen, mit denen Kunden, Mitarbeiter und andere betroffene Parteien über die Auswirkungen eskalierter Störfälle informiert werden. Im Notfall beruhigen diese Kommunikationsentwürfe sowohl innerhalb als auch außerhalb des Unternehmens die Gemüter.
In diesem Kapitel erfahren Sie, wie Sie den Plan überprüfen und die Unterstützung wichtiger Stakeholder im Unternehmen einholen.

Vorbereiten der einzelnen Akteure

Ein effektiver Incident Response Plan sollte das akzeptierte Risikoniveau der Organisation berücksichtigen und Vorbereitungen für die wahrscheinlichsten Bedrohungen für Ihr Unternehmen und Ihre Branche treffen.

Wird beispielsweise kein ausreichender Fokus auf die Sicherheitsfunktion gelegt, sollte der Incident Response Plan diese Schwachstelle aufdecken. Da das Team in diesem Fall nur begrenzt befähigt ist, einen zielgerichteten Angriff zu erkennen, empfiehlt es sich, vorrangig opportunistische, nicht zielgerichtete Bedrohungen zu bekämpfen.

Nachdem die wahrscheinlichsten Angriffe in Ihren IRP aufgenommen wurden, können die Rollen genauer definiert werden. Wichtige Ressourcen, die in Ihrem Plan noch fehlen, sollten nun hinzugefügt und entsprechend informiert werden. Sprechen Sie mit der Geschäftsleitung, Stakeholdern und Kollegen außerhalb der Sicherheitsfunktion: „Können Sie diese Reaktionen unterstützen? Was muss dafür erledigt werden?“

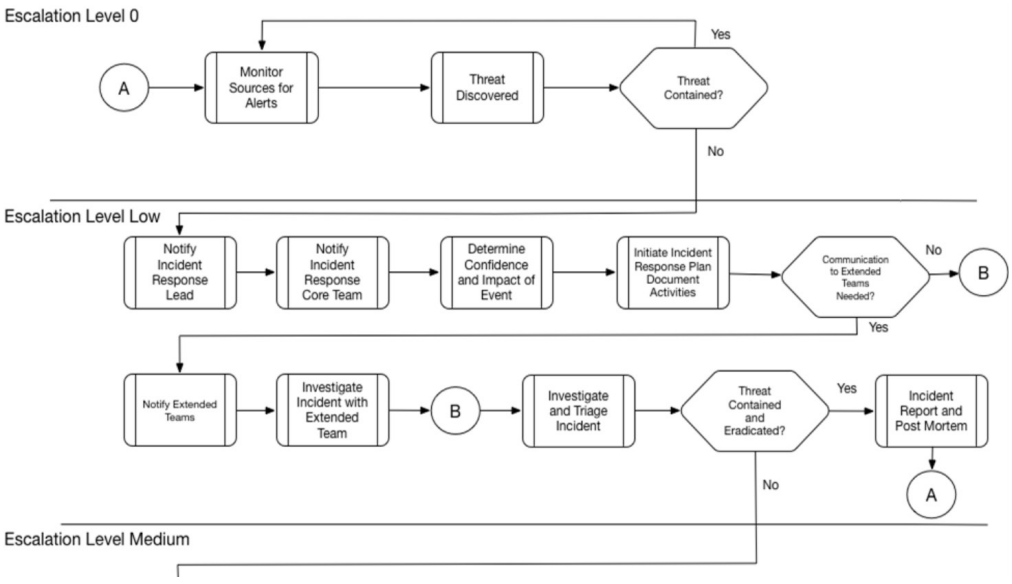
Stellen Sie in gemeinsamer Analysearbeit sicher, dass alle betroffenen Mitarbeiter – auch diejenigen außerhalb der Sicherheitsfunktion – ihre Rolle im Reaktionsworkflow verstehen.

Überprüfen von Prozessen und Protokollen

Stellen Sie sicher, dass alle Abteilungen wissen, wie sie eine vermutete Sicherheitsverletzung persönlich, via Telefon, E-Mail oder Kommunikationsanwendung melden können. Betrifft die Sicherheitsverletzung ein Kommunikationssystem (z. B. E-Mail), sollte die Meldung nicht über dieses System erfolgen.

Ein Priorisierungsworkflow hilft dem Sicherheitsteam dabei, Kontext aufzubauen und False-Positives zu eliminieren. Alle anderen funktionsübergreifenden Stakeholder benötigen klar definierte Prozesse, um eine Abwehr unterstützen zu können. Sie können damit besser einschätzen, an welchen Stellen eine höhere Eskalationsstufe erforderlich ist.

Unten: Beispielhafter Reaktionsworkflow auf niedriger Eskalationsstufe.

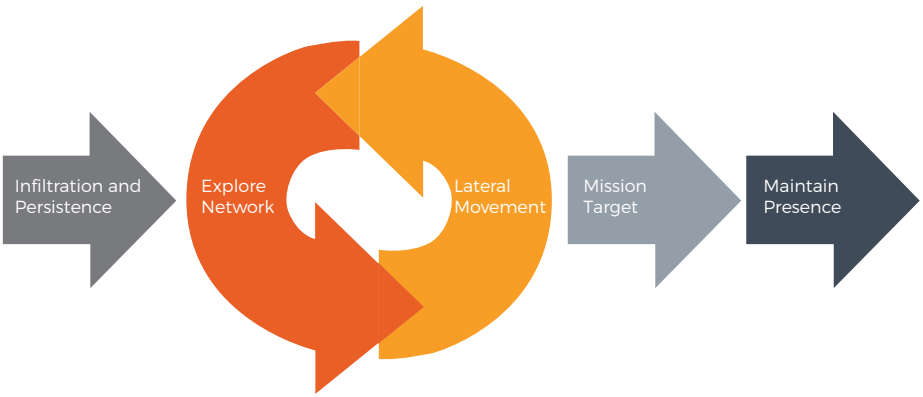


Im nächsten Schritt sollten alle Akteure die Protokolle für Kommunikationswege während eines Angriffs überprüfen. Definieren Sie beispielsweise alternative Kommunikationskanäle für den Fall einer Sicherheitsverletzung im primären Kanal, um die geplante Problembehebung vor Angreifern geheimzuhalten. Kommunizieren Sie nur essentielle Informationen, um unnötiges Gerede zu vermeiden.

Bestimmen Sie im Voraus, wie häufig kommuniziert werden soll. Eine allgemeine Panik und ständige Anfragen nach neuen Informationen sorgen nur für Frust und halten Ihr Team davon ab, den Störfall effizient zu bearbeiten.

Fehlersuche und flexible Anpassungen

An dieser Stelle sollte die Fähigkeit der Organisation, schädliches Verhalten zu erkennen, genau unter die Lupe genommen werden. Wir empfehlen dazu eine Zuordnung Ihrer Erkennungsfähigkeiten zur Angriffskette. Erstellen Sie zunächst ein Diagramm der einzelnen Schritte, die zum Eindringen in Ihre Organisation erforderlich sind.
Wie kann ein Angreifer beispielsweise nach der Kompromittierung der Cloud-Service- oder Endpunkt-Zugangsdaten eines mobilen Mitarbeiters Zugriff auf kritische interne Netzwerkassets erlangen?



Die Schritte in einer internen Angriffskette.

Die meisten Teams haben in den frühen Phasen der Angriffskette die größten Erkennungsprobleme. Selbst nach einer Zentralisierung der Sicherheitsdaten können Netzwerkscans, die Verwendung gestohlener Zugangsdaten und Lateral Movement (das Vorstoßen innerhalb des Netzwerks mithilfe von privilegierten Zugangsdaten) nur schwer erkannt werden.

Ihr Incident Response Plan sollte detailliert genug sein, um die häufigsten Sicherheitsverletzungen abzudecken, und dabei flexibel genug, um Anpassungen an veränderte Bedrohungen zuzulassen. Eine ständige Überprüfung und Anpassung an Veränderungen ermöglicht eine umfassende Eindämmung von Cyberangriffen.

Auch Ihre Abwehrfähigkeiten sollten wiederholt geprüft werden. Teams, die auftretende Sicherheitsverletzungen nicht effektiv untersuchen können, fühlen sich schnell überfordert und abgelenkt.

Einrichten regelmäßiger Überprüfungen

Überprüfungen sind am effektivsten, wenn sie in regelmäßigen Abständen erfolgen. Vierteljährliche Überprüfungen sind ideal, während Compliance-Standards mit expliziten IR-Plänen und jährlicher Zertifizierung mindestens eine Überprüfung pro Jahr vorschreiben. Stellen Sie bei der Überprüfung des IRP sicher, dass alle PR-Unterlagen die neuesten Änderungen widerspiegeln.

EINE STÄNDIGE ÜBERPRÜFUNG UND ANPASSUNG AN VERÄNDERTE BEDROHUNGEN ERMÖGLICHT EINE UMFASSENDE EINDÄMMUNG VON CYBERANGRIFFEN.

Mit einem Incident Response Plan sind Sie auf alle Eventualitäten vorbereitet. Optimal nutzen können Sie diesen allerdings erst nach einem eingehenden Test. So wie Krieger ihre Topform regelmäßigem Training verdanken, beruht auch ein erfolgreiches Abwehrmanagement auf mentaler Vorbereitung und in der Praxis eingeprägten Handgriffen.

SCHRITT 3: PLAN TESTEN

Sie haben nun den Incident Response Plan erstellt und ihn einer eingehenden Überprüfung unterzogen. Jetzt geht der Spaß erst richtig los!

Wenn Sie die richtige Mentalität entwickeln und sich die wichtigsten Handgriffe einprägen wollen, geht nichts ohne intensives Training.

Nachfolgend finden Sie verschiedene Möglichkeiten zum Testen Ihres IRP, sowie Vorschläge zur Beurteilung der Ergebnisse.

Tabletop-Übungen

Tabletop-Übungen stellen eine ausgezeichnete und stressarme Testmöglichkeit für Ihren IRP dar. In den meist halbtägigen Übungen wird die Reaktion eines funktionsübergreifenden Teams auf einen Angriff geübt. Auch wenn hierbei kein Störfall in Ihrem Netzwerk simuliert wird, sollte die Übung ernst genommen werden. Sie sollte als Generalprobe verstanden werden – nicht als Schulung oder Überprüfung des Incident Response Plan.

Eine erfolgreiche Übung steht und fällt mit ihrer Planung. Diese Fragen sollten dabei beantwortet werden:

- Wer soll an der Übung teilnehmen? Betrifft sie die Geschäftsleitung oder eher die Technik?
- Welches Szenario soll geübt werden? Ist es bezüglich der erwarteten Angriffsart (opportunistisch vs. zielgerichtet) und den aktuellen Abwehrfähigkeiten realistisch?
- Wie soll die Übung aufgebaut sein? Mithilfe eines einfachen Skripts und einer geplanten Abfolge können die Teilnehmer ihre Zeit optimal nutzen.

Red Team, Blue Team, Purple Team

Nach der Entwicklung eines grundlegenden Reaktionsworkflows im Rahmen der Tabletop-Übung folgt für Ihr Team der nächste Schritt.

Mitarbeiter der Sicherheitsfunktion, die sich mit Penetrationstests auskennen, können in Angriffssimulationen als Red Team und Blue Team gegeneinander antreten. Penetrationstests eignen sich perfekt zur Erforschung Ihrer Erkennungs- und Abwehrfähigkeiten sowie Ihrer koordinierten Angriffsreaktion.
Sie sollten sich nicht bloß auf technische Details konzentrieren, da eine umfassende Reaktion auf eine Sicherheitsverletzung die Unterstützung verschiedenster Funktionen erfordert.

So muss das Sicherheitsteam beispielsweise zunächst mit der IT kooperieren, um betroffene Geräte vom Netzwerk zu isolieren. Das PR-Team und andere Mitglieder der

EINE UMFASSENDE REAKTION AUF EINE SICHERHEITSVERLETZUNG ERFORDERT DIE UNTERSTÜTZUNG VERSCHIEDENSTER FUNKTIONEN.

Taskforce sollten Updates über einen festgelegten Kommunikationskanal erhalten. Häufigkeit und Detailgrad dieser Updates sollten im Vorfeld realistisch eingeschätzt und kommuniziert werden, damit das Team nicht durch ständige Fragen vom Reaktionsworkflow abgelenkt wird.

Angriff ohne Wenn und Aber

Je realistischer die Angriffssimulation, desto besser das Ergebnis. Wenn Sie Ihren Plan einem Penetrationstest durch eine externe Firma unterziehen, sollten Sie diese bei Erkennung im Netzwerk nicht informieren. Können Sie ihre Bewegungen nachverfolgen und schädliche Aktionen wie Rechteausweitungen oder Lateral Movement identifizieren?

An dieser Stelle sollten Sie auch alternative Kommunikationskanäle testen, um eine Kompromittierung des primären Kanals zu üben. Lassen Sie Ihr Team auf ungewohntem Terrain operieren. Gehen Sie an Ihre Grenzen, um Schwachstellen zu identifizieren.

Sichern Sie forensische Daten. Auch wenn Sie kompromittierte Geräte nach Erkennung eines Störfalls am liebsten sofort aus dem Netzwerk nehmen würden, kann es sinnvoll sein, ihren Betrieb zunächst aufrechtzuerhalten. Schließlich sollen wichtige forensische Beweise wie Systemspeicherdaten nicht verloren gehen.

Angemessene Dokumentation

Schriftliche Unterlagen und elektronische Beweise sind in der Zeit während und nach einem Angriff unverzichtbar. So können manipulierte Beweise vor

Gericht beispielsweise nicht zur Klärung der Schuldfrage zugelassen werden.
Incident-Response-Teams müssen deshalb eine zuverlässige Dokumentation aller Aktivitäten innerhalb der Organisation (wer, was, wann, warum) sicherstellen.

Anhand der Dokumentation lässt sich auch besser nachvollziehen, wie ein Angriff abgelaufen ist.

- Haben menschliche Handlungen oder Unterlassungen dazu beigetragen?
- Lag ein Defekt bzw. eine Fehlfunktion vor oder fehlten Komponenten?
- Könnte der Angriff – ob absichtlich oder durch bloße Nachlässigkeit – von einem Mitarbeiter verursacht worden sein?

Eine angemessene Dokumentation während der Abwehr eines Störfalls kann Sie bei der Beantwortung dieser Fragen unterstützen.

Erfolgskontrolle

Die Überprüfung wird mit einem „After Action Review“ abgeschlossen. Ihre Organisation kann damit den Erfolg einzelner Prozessschritte beurteilen und den Plan an gewonnene Erkenntnisse anpassen, um gegen zukünftige Angriffe besser gewappnet zu sein.

Für eine erfolgreiche Überprüfung müssen die wahren Risiken identifiziert und ihre Behandlung (oder auch ihre Akzeptanz) ehrlich erfasst werden. Ein zuverlässiger Plan muss sich kontinuierlich weiterentwickeln, um mit neuen Angriffsvektoren und einem sich stetig veränderndem Netzwerk umgehen zu können.

Testen Sie Ihren Plan anhand dieser drei Orientierungspunkte:

- Beurteilen Sie die aktuellen Erkennungs- und Abwehrfähigkeiten.
- Erarbeiten Sie konkrete Verbesserungsvorschläge.
- Erweitern Sie die Bandbreite der Störfälle, die sich das Team zutrauen kann.

Im Rahmen dieser Post-mortem-Analyse können Sie neu bewerten, welche Simulations-, Erkennungs- oder Abwehrschritte intern am besten funktionieren und welche von externer Unterstützung profitieren könnten.

Die beschriebenen Plan- und Testaktivitäten sind zwar umfangreich, machen sich aber besonders im Falle einer eskalierten Sicherheitsverletzung schnell bezahlt.

Im letzten Kapitel erfahren Sie, wie Ihre Organisation mit gravierenden Angriffen umgehen und auch in der Hitze des Gefechts einen kühlen Kopf bewahren kann.

SCHRITT 4: IM FALLE EINER SICHERHEITS-VERLETZUNG

Die folgenden Empfehlungen helfen Ihnen bei der Reaktion auf einen echten Störfall. Sie gelten sowohl für eskalierte opportunistische Angriffe als auch für die seltenen, aber durchaus realen zielgerichteten Bedrohungen.

Ganz wichtig: Sie, Ihr Team und die Mitarbeiter Ihres Unternehmens spielen bei der Reaktion auf einen Störfall die zentrale Rolle. Angreifer sind Menschen, angetrieben von Motiven, Zielen und einer günstigen Gelegenheit. Eine erfolgreiche Abwehr ist nur möglich, wenn Sie ruhig bleiben und sich nicht durch Wut, Hilflosigkeit oder Angst von einer koordinierten Reaktion abhalten lassen.

SIE, IHR TEAM UND DIE MITARBEITER IHRES UNTERNEHMENS SPIELEN BEI DER REAKTION AUF EINEN STÖRFALL DIE ZENTRALE ROLLE.

Atmen Sie tief ein und wieder aus. Und holen Sie sich Hilfe.

In vielen Fällen entdeckt ein Mitglied des IT- oder Sicherheitsteams den Störfall in Form von verdächtigen Aktivitäten in Ihrem Netzwerk. Je nachdem, über welche Erkennungsfähigkeiten Sie verfügen, kann es sich dabei beispielsweise um auffällige Netzwerkscans oder später in der Angriffskette um ungewöhnlich viele externe Verbindungen handeln, die auf Datenexfiltration hinweisen.

Befolgen Sie unabhängig von der Art des Störfalls den Plan und informieren Sie den Leiter der IT-Sicherheit oder Ihren Sicherheitsmanager. Ihr Hauptziel besteht

zunächst darin, Kontext aufzubauen und die potenziellen Auswirkungen des Störfalls zu identifizieren.

Kontext und Ausmaß der Auswirkungen

Definieren Sie die Störfallparameter, indem Sie die W-Fragen (wer, was, wo) rund um das schädliche Verhalten beantworten. Trat die verdächtige Aktivität beispielsweise auf einem bestimmten Asset wie einem Server auf, gilt es Folgendes zu prüfen:

- Inwieweit ist dieses Asset geschäftskritisch?
- Welche authentifizierten Benutzer haben Zugriff darauf? Können diese Benutzer privilegierte Handlungen ausführen?
- Sammelt Ihr SIEM-System Endpunktdaten für zusätzlichen Kontext?

Vermuten Sie dagegen kompromittierte Zugangsdaten, überlegen Sie Folgendes:

- Über welche Adminrechte verfügt dieser Benutzer?
- Ist sich der Benutzer des Vorfalls bewusst?
- Was passiert auf den entsprechenden Benutzerkonten?

Wenn sich Ihr Team proaktiv mit dem Ausgangszustand des Unternehmensnetzwerks vertraut macht, kann die Störfallschwere später schneller eingeschätzt werden. Andernfalls erweist sich die Feststellung, ob eine Meldung durch einen falsch konfigurierten Laptop, das BYOD-Gerät eines Entwicklers oder einen tatsächlichen Angriff mittels kompromittierter Zugangsdaten verursacht wurde, als schwierig.

Ein Priorisierungsworkflow verhindert, dass die Geschäftsleitung durch eine false-positive Meldung unnötigerweise alarmiert wird. Haben Sie Ihren IRP dagegen getestet und eskalieren nur im Falle einer tatsächlichen Sicherheitsverletzung, so können Sie meist mit der vollen Aufmerksamkeit der Geschäftsleitung rechnen.

Sichern von Beweisen

Forensische Beweise können schnell durcheinander geraten. Dabei sollten sie nicht nur Ihrer Organisation, sondern auch externen IR- und Rechtsberatern, die Sie in den Reaktionsworkflow einbeziehen, möglichst unverändert zur Verfügung stehen.

Achten Sie deshalb darauf, dass unbeständige Beweise wie z. B. Datenspeicher intakt bleiben. Wenn Sie kompromittierte Systeme in einem Anflug von Panik einfach ausschalten, warnen Sie damit nicht nur den Angreifer, sondern vernichten womöglich auch wichtige Beweise.

Bestimmen Sie schon im Vorfeld einen Mitarbeiter in Ihrer Organisation mit forensischem Fachwissen und nehmen Sie die entsprechenden Kontaktdaten in den Incident Response Plan auf.

Externe IR-Partner sollten, sofern vorhanden, so früh wie möglich kontaktiert werden. Wir bei Rapid7 werden beispielsweise lieber wegen einer harmlosen Aktivität angerufen, als zu riskieren, dass sich die Reaktion auf einen schwerwiegenden Störfall verzögert.

Durch das frühzeitige Einbinden externer Partner profitieren Sie von neuen Perspektiven und können mit vereinten Kräften die optimale Behebungsstrategie identifizieren und ausführen. IR-Dienstleister verfügen außerdem über die nötige Erfahrung, um Ihr Team bei rechtlichen Fragen zu unterstützen und gemeinsam gefährliche Stolperfallen zu umgehen.

Rechtsberatung

Bei Störfällen, die Kundendaten und Compliance-Verstöße betreffen, sollten Sie frühzeitig einen Rechtsberater einschalten. Ihre Maßnahmen in der frühen Reaktionsphase können später regulatorisch und rechtlich unter die Lupe genommen werden.
Haben Sie schnell und angemessen reagiert? War ein nachlässiger Mitarbeiter an dem Vorfall beteiligt? Gab es einen Hardwaredefekt oder Schwachstellen in bereitgestellter Software? All diese Fragen könnten später Teil einer Untersuchung werden. Ein Rechtsberater kann Ihnen dabei helfen, sie zu beantworten.

Auch die ausgesprochen wichtige Reaktion Ihres PR-Teams kann von den Hinweisen des Rechtsberaters profitieren. Laut einem Artikel im Harvard Business Review können selbst Gerüchte um eine Sicherheitsverletzung großen Schaden anrichten. Zur Vorbeugung einer PR-Krise sollten Sie deshalb mit klarer und direkter Kommunikation an die Öffentlichkeit treten.

WENDEN SIE SICH AN EINEN INCIDENT RESPONSE PARTNER

Neben Tipps zur Formulierung der perfekten Pressemitteilung erfährt das PR-Team von einem Rechtsberater außerdem, welche Details zu einem Störfall gesetzlich veröffentlicht werden müssen. Auch hier zeigt sich die Bedeutung einer engen Zusammenarbeit zwischen technischen und anderen Teams.

Planausführung

Halten Sie sich an Ihren Plan. Dafür haben Sie ihn eingeübt. Machen Sie sich aber auch bewusst, dass jeder Störfall einzigartig ist und Abweichungen erforderlich sein können. Stellen Sie sicher, dass diese Abweichungen gerechtfertigt sind und umfassend dokumentiert werden.

Unabhängig von den Umständen der jeweiligen Krisensituation wird sich das ausführliche Entwerfen, Prüfen und Testen einer soliden Grundlage für schnelle, differenzierte Reaktionen für Sie, Ihre Organisation und Ihre externen Sicherheitspartner auszahlen.

Grundvoraussetzung für einen effektiven Incident Response Plan ist Transparenz bezüglich Netzwerk, Assets, Schwachstellen und Bedrohungen.

Ein zuverlässiger IR-Partner kann Sie unter anderem in den folgenden Bereichen unterstützen:

- Erkennungs- und Abwehrtechnologie
- MDR-Dienste (Managed Detection and Response)
- Angriffssimulation: Tabletop- und Red/Blue-Team-

Übungen

- Incident-Response-Dienste

Jede Organisation hat individuelle Prioritäten und Bedürfnisse. Stellen Sie deshalb sicher, dass bei der Wahl des IR-Partners alle an einem Strang ziehen.

Mit InsightIDR von Rapid7 können Organisationen ihre Daten zusammenführen, Angriffe frühzeitig erkennen und Risiken durch den Einsatz von Sicherheitsanalytik priorisieren. Unsere Incident-Response-Dienste helfen Teams bei der proaktiven Vorbereitung und dem Ausbau interner Fähigkeiten.

Besuchen Sie rapid7.com, um mehr über unsere Produkte und Dienste zu erfahren und unsere Technologie kostenlos zu testen.

ANHANG

Incident-Response-Kontakte

Notfallkontaktdaten

- Incident-Response-Kontakte
- Incident-Response-Drittkontakte
- Betroffene Drittkontakte

Rollen und -Verantwortlichkeiten Incident Response

TEAMROLLEN INCIDENT RESPONSE UND KONTAKTDATEN

Rolle	Kontaktname	Kontaktdaten
Leiter Incident Response Agiert als Verbindung zwischen IT & Geschäftseinheiten. Erstellt und dokumentiert Updates für die Geschäftsleitung.		Büro: Mobil: E-Mail:
Koordinator Incident Response Gewährleistet die ordnungsgemäße Durchführung des IRP. Validiert die Untersuchung, Eindämmung, Behebung und Wiederherstellung.		Büro: Mobil: E-Mail:
Leiter Rechtsfragen Bewertet Haftungen und Verpflichtungen während und nach einem Störfall. Koordiniert die Kommunikation mit Behörden und der Öffentlichkeit.		Büro: Mobil: E-Mail:
Leiter Investor Relations Verfasst und kommuniziert Updates bezüglich Störfall, Status und Abschluss an Investoren.		Büro: Mobil: E-Mail:
Leiter Public Relations Kommuniziert Ereignisse in geeigneter Form an die Öffentlichkeit. Empfiehlt Zeitpunkt und Verbreitung.		Büro: Mobil: E-Mail:
Leiter Interne Kommunikation Verfasst und kommuniziert interne Updates zum Störfall. Informiert Behörden und interessierte Parteien gemäß Verpflichtungen.		Büro: Mobil: E-Mail:
Leiter IT-Betrieb Ist für den gesamten System-/Anwendungsbetrieb verantwortlich. Verwaltet die technischen Aspekte der Abwehr und Wiederherstellung.		Büro: Mobil: E-Mail:
Leiter IT-Sicherheit Gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit von Informationsassets. Agiert als Verbindung zwischen externen Experten (z. B. Rapid7) und dem internen IR-Team.		Büro: Mobil: E-Mail:
Leiter Schadensprävention Gewährleistet den Schutz materieller Assets. Agiert als Verbindung zur Polizei und gewährleistet die Sicherung relevanter Daten in enger Zusammenarbeit mit der IT.		Büro: Mobil: E-Mail:
Leiter Auditierung Dokumentiert eventuelle Probleme mit dem Incident Response Prozess. Gewährleistet die vollständige Bearbeitung der erforderlichen Schritte, Formulare und Dokumente.		Büro: Mobil: E-Mail:

NOTFALLKONTAKTDATEN

INCIDENT-RESPONSE-KONTAKTE

Kontakte zur Störfallmeldung	
Kommunikationskanal	Kontaktdaten
Anruf Geschäftsleitung	
Anruf Technik	
E-Mail	
Sonstiges	

Behördenkontakte		
Rolle	Partei	Kontaktdaten
Handelsbank	Partei	
Staatspolizei	Kontaktdaten	
Staatspolizei	Polizeibehörde	
BSI	Lokale Verwaltungsstelle	
Geheimdienst	Lokale Verwaltungsstelle	

INCIDENT-RESPONSE-DRITTKONTAKTE

Incident-Response-Drittkontakte		
Rolle	Partei	Kontaktdaten
Incident-Response-Experte	Rapid7	844.RAPID.IR
Kreditschutzorganisation	Kreditschutzorganisation	
PR-Agentur	PR-Agentur	
Externe Rechtsberatung	Anwaltskanzlei	

BETROFFENE DRITTKONTAKTE

Hotlines zur Störfallmeldung		
Betroffene Partei	Kontaktname	Kontaktdaten
Kundenname		
Lieferantenname		
Fachkollege		
Informationseigentümer		

ROLLEN UND VERANTWORTLICHKEITEN INCIDENT RESPONSE

TEAM	VERANTWORTLICHKEITEN
LEITER INCIDENT RESPONSE	A. Störfallkoordination B. Bestätigung Störfallfeststellung und -schwere C. Bestätigung Störfallbehebung D. Koordination der Störfallkommunikation E. Beauftragung externer technischer Experten
INCIDENT RESPONSE TEAM / SICHERHEITSBETRIEB	A. Sicherheitsüberwachung/Störfallerkennung B. Störfallfeststellung C. Störfallnachverfolung und -dokumentation D. Durchführung der Incident-Response-Aktivitäten E. Störfallbehebung F. Technische Analyse G. Forensische Analyse (falls intern durchgeführt)
RECHTSTEAM / ALLGEMEINE BERATUNG	A. Koordination mit Justizbehörden B. Beauftragung externer Beratung C. Prüfung der relevanten Störfallkommunikation
LEITER PUBLIC RELATIONS	A. Autorisierung und Durchführung der Kommunikation mit externen Parteien B. Beauftragung von PR-Agentur
LEITER INTERNE KOMMUNIKATION	A. Autorisierung und Durchführung der Kommunikation mit internen Parteien / Unternehmensmitarbeitern
LEITER INVESTOR RELATIONS	A. Autorisierung und Durchführung der Kommunikation mit Unternehmensstakeholdern
LEITER IT-SICHERHEIT/-BETRIEB	A. Planung von Behebung und Wiederherstellung B. Koordination von Begrenzungs- und Behebungsmaßnahmen
LEITER SCHADENSPRÄVENTION	A. Beauftragung von Kreditschutzorganisation
DESKTOP-SUPPORT	A. Desktop-/Laptop-Support B. Unterstützung technischer Untersuchungen C. Eindämmung D. Systemwiederherstellung
NETZWERKBETRIEB	A. Netzwerküberwachung B. Protokollauswertung C. Unterstützung technischer Untersuchungen D. Eindämmung E. Systemwiederherstellung

Anmerkung: Bei dieser Teamaufstellung handelt es sich lediglich um ein Beispiel. Der tatsächliche Aufbau der einzelnen Teams variiert mit der Unternehmensstruktur.

ROLLEN UND VERANTWORTLICHKEITEN INCIDENT RESPONSE (FORTS.)

TEAM	VERANTWORTLICHKEITEN
DATENBANK	A. Datenbankanalyse B. Protokollauswertung C. Unterstützung technischer Untersuchungen D. Eindämmung E. Systemwiederherstellung
SERVER	A. Serveranalyse B. Protokollauswertung C. Unterstützung technischer Untersuchungen D. Eindämmung E. Systemwiederherstellung
ANWENDUNGSTEAMS	A. Anwendungsanalyse B. Protokollauswertung C. Unterstützung technischer Untersuchungen D. Eindämmung E. Systemwiederherstellung

Anmerkung: Bei dieser Teamaufstellung handelt es sich lediglich um ein Beispiel. Der tatsächliche Aufbau der einzelnen Teams variiert mit der Unternehmensstruktur.

ÜBER RAPID7

Rapid7 (NASDAQ: RPD) verleiht zahlreichen Sicherheits- und IT-Experten das Verständnis und das nötige Selbstvertrauen, um Risiken abzuwehren und Innovation voranzutreiben. Unsere Analytik wandelt Daten in wichtige Erkenntnisse um, die unseren Kunden dabei helfen, Schwachstellen zu beseitigen und anspruchsvolle IT-Infrastrukturen, Netzwerke und Anwendungen sicher zu entwickeln und zu betreiben. Die Lösungen von Rapid7 umfassen Schwachstellenmanagement, Penetrationstests, Anwendungssicherheit, Störfallerkennung und -abwehr, SIEM und Protokollmanagement. Weiterhin bietet Rapid7 Managed Services und Beratungsdienste zum gesamten Portfolio.

Weitere Informationen über Rapid7 und unsere Bedrohungsforschung finden Sie unter **www.rapid7.com.**

RAPID7