eBook

Warum Sie einen Vorfallsreaktion-splan brauchen

exabeam™

Inhaltsverzeichnis

Warum Sie einen Vorfallsreaktionsplan brauchen

Einführung

Warum Sie einen Vorfallsreaktionsplan brauchen

Im Laufe des nächsten Jahres werden die meisten Unternehmen mit einem schwerwiegenden Sicherheitsvorfall konfrontiert sein, oder schlimmer noch, mit einer Datenschutzverletzung oder einem Ransomware-Angriff. Der 2021 Data Breach Investigations Report von Verizon hob 29.207 Sicherheitsvorfälle in Unternehmen allein im letzten Jahr hervor. Laut dem Identity Theft Resource Center gab es in den USA vom 1. Januar bis zum 30. September 2021 1.291 öffentlich gemeldete Datenschutzverletzungen, das sind 17 % mehr als im gesamten Jahr 2020. Diese Zahlen schließen Vorfälle aus, bei denen die Unternehmen nicht zur Meldung verpflichtet waren oder nicht einmal wussten, dass etwas vorgefallen war.

In den Fällen, in denen Unternehmen nicht wissen, dass sie verletzt wurden, erfahren sie es oft von einem Dritten, z. B. einem Kunden, einer Strafverfolgungsbehörde, einem Finanzinstitut oder einem Partner in der Lieferkette. Im Falle von Ransomware erfahren sie dies durch Bildschirmmitteilungen und unzugängliche, verschlüsselte Daten. Zu diesem Zeitpunkt fällt es vielen schwer, das Ausmaß und den Ursprung eines Vorfalls oder einer Datenschutzverletzung zu identifizieren.

49%

Fast die Hälfte der Sicherheitsleiter gibt an, dass es ihrem Unternehmen an adäquaten Tools fehlt, um Bedrohungen zu verhindern, zu erkennen oder darauf zu reagieren.

8%

der Sicherheitsleiter sind zuversichtlich, dass sie den Ursprung eines Vorfalles identifizieren könnten.

Abbildung 01 Ungefähr die Hälfte (49 %) der Sicherheitsleiter gibt an, dass es ihrem Unternehmen an adäquaten Tools fehlt, um Bedrohungen zu verhindern, zu erkennen oder darauf zu reagieren. Nur 8 % der Sicherheitsleiter sind zuversichtlich, dass sie den Ursprung eines Vorfalles identifizieren könnten. (Bildquelle)

Wenn es zu Vorfällen kommt, stehen die Sicherheitsteams unter enormem Druck. In einer derart hektischen Umgebung befolgen sie möglicherweise nicht die richtigen Verfahren zur Vorfallsreaktion, um den Schaden zu begrenzen. In Ermangelung

der richtigen Informationen oder eines formellen Plans reagieren viele über, schalten zu viele Systeme ab oder patchen sie und unterbrechen den Betrieb auf eine Weise, die das Geschäftsrisiko vergrößert. In manchen Fällen können durch eine übereilte Reaktion wertvolle forensische Informationen verloren gehen, die benötigt werden, um einen Angriff zu isolieren und zu beseitigen.

Um schneller, effizienter und konsequenter auf Vorfälle zu reagieren, sollten sich CISOs, IT-Mitarbeiter und andere Sicherheitsexperten auf einen Vorfallsreaktionsplan verlassen. Zu viele Unternehmen versäumen es, diesen wichtigen Schritt zu tun. Wie Sie der Grafik auf der rechten Seite entnehmen können, geben 64 % der Sicherheitsverantwortlichen an, dass ihr Unternehmen über eine strukturierte Vorfallsreaktion verfügt, was bedeutet, dass 36 % ohne Fallschirm fliegen.

Gehen Sie nicht davon aus, dass Vorfallsreaktionspläne nur etwas für große, etablierte Unternehmen sind. Unternehmen jeder Größe und jedes Reifegrads sind mit schwerwiegenden Sicherheitsvorfällen konfrontiert, die wirksam gehandhabt werden müssen. Im Bericht von Verizon für das Jahr 2021 wurden mehr als 45 % der Sicherheitsverletzungen in Unternehmen mit weniger als 1.000 Mitarbeitern verzeichnet.

Im Folgenden erfahren Sie, warum ein Vorfallsreaktionsplan ein wichtiger Bestandteil Ihrer Cybersicherheitsstrategie sein sollte. Dieses E-Book enthält einige wertvolle Richtlinien und Tipps, die CISOs und Incident Responder zum Erfolg führen.

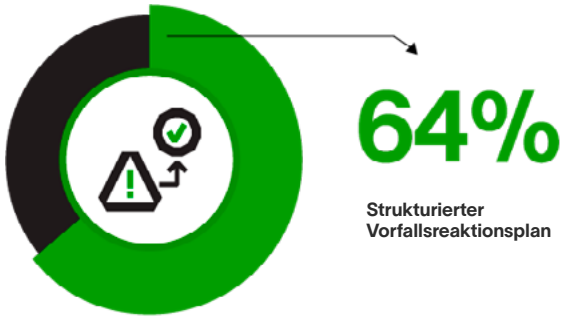


Abbildung 02 64 % der Sicherheitsverantwortlichen geben an, dass ihr Unternehmen über einen strukturierten Vorfallsreaktionsplan verfügt. (Bildquelle)

Was ist ein Vorfallsreaktionsplan?

Vorfallsreaktion (Incident Response, IR) ist eine strukturierte Methodik für den Umgang mit Sicherheitsvorfällen, Datenschutzverletzungen und Cyber-Bedrohungen. Ein Vorfallsreaktionsplan ist ein lebendiges Dokument, das jährlich (und nach jedem Vorfall) bewertet, getestet und überarbeitet werden muss, um einen anhaltenden Nutzen zu bieten. Ein gut ausgearbeiteter Vorfallsreaktionsplan (IRP) ermöglicht es Ihnen:

- **Einen Vorfall, eine Datenschutzverletzung oder eine Cyber-Bedrohung zu identifizieren**
- **Dessen Umfang und Auswirkungen zu verstehen**
- **Kosten und andere Schäden zu minimieren**
- **Effektiv mit internen und externen Parteien und der Öffentlichkeit zu interagieren**
- **Die Ursache zu beheben**
- **Den Betrieb wiederherzustellen**
- **Aus dem Angriff zu lernen und Ihre Sicherheitsmaßnahmen zu verbessern**

Es gibt viele Leitfäden und Vorlagen für Vorfallsreaktionspläne, einschließlich des bekannten 2012 Computer Security Incident Handling Guide des US-amerikanischen National Institute of Standards and Technology (NIST). Diese – ebenso wie dieser Leitfaden – sollten jedoch lediglich als eine Sammlung allgemein anerkannter bewährter Verfahren betrachtet werden. Es ist von entscheidender Bedeutung, dass jedes Unternehmen einen Plan erstellt, der auf sein Geschäft, seine kritischen Systeme, seine Sicherheitsumgebung und seine Kultur zugeschnitten ist. Es ist außerdem wichtig, dass der Plan klare, auf die jeweilige Umgebung zugeschnittene Verfahren sowie klar definierte Rollen, Verantwortlichkeiten und Kommunikationskanäle spezifiziert.

Viele Unternehmen arbeiten mit einer Kombination aus Bewertungs-Checklisten, detaillierten Vorfallsreaktionsplänen, direkt umsetzbaren Playbooks für die Vorfallsreaktion und Richtlinien, um einen Teil der Prozesse zu automatisieren.

Manche Sicherheitsanbieter können Ihnen bei den ersten Schritten dafür behilflich sein. Denken Sie daran, nach ihnen zu fragen.

Gehen Sie sicher, dass alle Vorfallsreaktionspläne und Überarbeitungen von der Geschäftsleitung genehmigt werden. Sie möchten keine kostbare Zeit damit verbringen, zu warten oder, schlimmer noch, während eines Sicherheitsvorfalls um die Genehmigung zu kämpfen, wenn die Zeit nicht auf Ihrer Seite ist.

Bewahren Sie aktuelle gedruckte Exemplare des gesamten Vorfallsreaktionsplans auf, für den Fall, dass Sie während eines Vorfalls, wie z. B. im Falle von Ransomware, den Zugriff auf die digitale Version verlieren.

Meldung von Sicherheits-verletzungen – Wann, wann nicht und warum.

Wenn eine Cybersicherheitsverletzung von Sicherheitsanalysten bestätigt wird, ist es wichtig, dass Sie Ihre Meldepflichten kennen. Nicht alle Sicherheitsverletzungen müssen gemeldet werden.

Achten Sie darauf, dass Sie Ihrem Rechtsbeistand die richtigen Fragen stellen. Bei Verstößen, die eine Benachrichtigung erfordern, informieren Sie die betroffenen Parteien so schnell wie möglich.

Datenschutzgesetze wie die DSGVO und der kalifornische CCPA verlangen häufig eine öffentliche Benachrichtigung und in einigen Fällen eine persönliche Benachrichtigung der betroffenen Personen. Auch börsennotierte Unternehmen unterliegen bestimmten Offenlegungspflichten, stellen Sie also sicher, dass Sie diese dokumentieren.

Je nach Schwere der Verletzung sollten die Rechts- und Presseabteilung sowie die Geschäftsleitung einbezogen werden. In vielen Fällen müssen andere Abteilungen wie der Kundendienst, die Finanzabteilung, die PR- oder die IT-Abteilung sofort tätig werden. Ihr Vorfallsreaktionsplan sollte je nach Art und Schwere der Datenschutzverletzung klar angeben, wer informiert werden sollte. Der Plan muss die vollständigen Kontaktdaten und die genaue Kommunikation mit allen relevanten Parteien enthalten, um nach einem Angriff Zeit zu sparen.

Ereignis, Vorfall oder Sicherheitsverletzung?

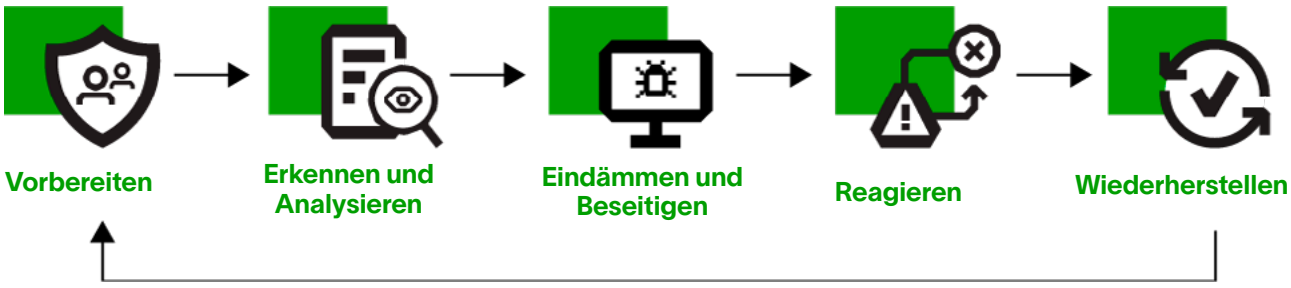
Ereignis: Laut NIST ist ein Ereignis jedes beobachtbare Vorkommnis in einem System oder Netzwerk (oder heute in einer Cloud-Instanz). Ein unerwünschtes Ereignis ist ein Ereignis, das eine negative Konsequenz hat, wie z. B. die unbefugte Nutzung von Systemprivilegien oder die Ausführung von Malware, die Daten zerstört. Eine andere Möglichkeit, ein Ereignis zu definieren, ist jede Änderung des „normalen" digitalen Verhaltens eines Systems, Prozesses oder Benutzers.

Vorfall: Laut dem DBIR von Verizon ist ein Vorfall ein Sicherheitsereignis, das die Integrität, Vertraulichkeit oder Verfügbarkeit eines Informationsgutes gefährdet.

Sicherheits- bzw. Datenschutzverletzung: Ein Vorfall, der zu einer bestätigten – und nicht nur potenziellen – Offenlegung von Daten gegenüber einer nicht autorisierten Partei führt.

Die 5 Schritte eines umfassenden Vorfallsreaktionsplans

Keine zwei Vorfallsreaktionspläne sind gleich, und Ihr Plan sollte speziell auf Ihr Unternehmen zugeschnitten sein. Die meisten umfassen die folgenden Schritte:



Vorbereiten: Planen Sie im Voraus, wie Sie Sicherheitsvorfälle verhindern und handhaben.

Erkennen und Analysieren: Überwachen Sie potenzielle Angriffsvektoren und identifizieren, priorisieren und bestimmen Sie das Ausmaß und den Ursprung eines Vorfalls.

Eindämmen und Beseitigen: Entwickeln Sie eine Strategie zur Eindämmung des Vorfalls und identifizieren bzw. schützen Sie die angegriffenen Hosts und Systeme.

Reagieren: Interagieren Sie konstruktiv mit Strafverfolgungsbehörden, Kunden, anderen Stakeholdern und den Medien auf eine Art und Weise, die wahrheitsgemäß ist, aber den Schaden für das Unternehmen und die Marke minimiert.

Wiederherstellen: Testen und rezertifizieren Sie die betroffenen Systeme als sicher. Aktivieren Sie sie in der Produktionsumgebung. Werten Sie die gewonnenen Erkenntnisse aus und nehmen Sie die notwendigen Änderungen an Ihren Sicherheitsrichtlinien, Ihrem Programm und Ihrem Vorfallsreaktionsplan vor.

1. Vorbereiten

Die Vorbereitung auf Sicherheitsvorfälle umfasst mehrere Schritte, von denen der erste die Zusammenstellung eines Computer Security Incident Response Teams (CSIRT) ist. Es ist von entscheidender Bedeutung, die richtigen Mitarbeiter mit den richtigen Fähigkeiten und der entsprechenden Expertise im Team zu haben.

Das Team zusammenstellen

In kleineren Unternehmen oder wenn eine Bedrohung nicht allzu schwerwiegend ist, können Ihr SOC- oder IT-Team bzw. Ihre Managed Security Consultants ausreichend sein, um einen Vorfall zu bewältigen. In den meisten größeren Unternehmen sollte ein CSIRT-Team aus den folgenden Mitgliedern bestehen.

TeamleiterIn / BefehlshaberIn

Normalerweise jemand aus dem Bereich Sicherheit/IT, der die Gesamtverantwortung für die Reaktion auf einen Vorfall trägt. Diese Person sollten einen direkten Draht zur Geschäftsleitung haben, damit wichtige Entscheidungen – wie z. B. das Abschalten wichtiger Systeme – schnell getroffen werden können.

Leitende/r ErmittlerIn

Jemand aus Ihrem SOC/IT-Team (kleinere Unternehmen) oder ein Managed Security Consultant, der für die Verwaltung der Beweise für einen Vorfall und die Leitung von Sicherheitsanalysten und anderen IT-Mitarbeitern verantwortlich ist, die an der Ursachenanalyse, Eindämmung, Beseitigung und Systemwiederherstellung beteiligt sind.

Kommunikations beauftragte/r

Oft aus der Abteilung für Öffentlichkeitsarbeit oder Unternehmenskommunikation des Unternehmens, die für die Erstellung der angemessenen Botschaften für alle Interaktionen mit Mitarbeitern, Kunden, Medien und der Öffentlichkeit verantwortlich ist.

Personal- / juristische/r Beauftragte/r

Stellt Expertenwissen zu regulatorischen und rechtlichen Fragen sowie zu notwendigen öffentlichen Mitteilungen, Rechtsstreitigkeiten, Strafanzeigen oder internen Maßnahmen gegen bestimmte Mitarbeiter bereit.

Dokumentations leiterIn

Dokumentiert jeden einzelnen Schritt der Vorfallsreaktion, die Zeitachse des Vorfalls und alle Details zur Entdeckung und Reaktion auf den Vorfall sowie zur anschließenden Wiederherstellung.

Sie müssen eine Führungskraft im Team haben, damit alle Entscheidungen, die sich auf das Geschäft auswirken, sofort getroffen werden können.

Es ist wichtig, dass der Plan die Ziele dieses Teams, die Situationen, in denen es kontaktiert und zusammengerufen werden sollte (und wann nicht) sowie die spezifischen Verantwortlichkeiten jedes Teammitglieds sehr detailliert beschreibt.

Beziehen Sie ALLE Kontaktdaten der einzelnen Teammitglieder ein, sowohl am Arbeitsplatz als auch zu Hause, und wie diese am besten zu erreichen sind, wenn sie gerade im Urlaub oder unterwegs sind.

Weitere Vorbereitungsschritte

Die Vorbereitungsphase ist außerdem der richtige Zeitpunkt für Folgendes:

Assets priorisieren: Bestimmen Sie, welche Anwendungen, Server, Datenbanken und andere IT-Komponenten für das Unternehmen von entscheidender Bedeutung sind. Entwickeln Sie ein Verständnis vom normalen und abnormalen Verhalten dieser Systeme. Machen Sie sich mit ihren privilegierten Benutzern vertraut. Entwickeln Sie ein Verständnis der Arten von Angriffen, mit denen Unternehmen in Ihrer Branche am wahrscheinlichsten konfrontiert sehen.

Stakeholder identifizieren: Sammeln Sie die Kontaktinformationen Ihrer Kunden – insbesondere Ihrer strategisch wichtigsten Kunden – und aller anderen Stakeholder, für die eine Sicherheitsverletzung erhebliche finanzielle oder rechtliche Auswirkungen hätte. Sie möchten nicht in der Hitze des Gefechts nach diesen Informationen suchen müssen und feststellen, dass Sie sie nicht haben.

Entwickeln Sie Beziehungen zu den Strafverfolgungsbehörden: Bringen Sie in Erfahrung, wen in den lokalen und anderen Strafverfolgungsbehörden Sie im Falle eines schwerwiegenden Vorfalls oder einer Datenschutzverletzung kontaktieren werden. Halten Sie

alle Kontaktinformationen fest, stellen Sie die relevanten Teammitglieder vor und bauen Sie eine Beziehung auf, damit Sie schnell mit Ihren Ansprechpartnern bei den Strafverfolgungsbehörden zusammenarbeiten können, falls oder wenn es soweit ist.

Develop a communications plan: Dies ist die Art und Weise, auf die Unternehmensvertreter intern und mit Kunden, Stakeholdern, Medien und der Öffentlichkeit interagieren werden. Inkompetente Kommunikation ist eine der Hauptursachen für ernsthafte Markenschädigungen.

Sie möchten nicht, dass Ihre Vertreter schädliche Falschaussagen machen oder unter Druck nicht angemessen kommunizieren können. Eine gute Praxis ist es, eine Liste mit roten und grünen Aussagen zu erstellen: grün für das, was Sprecher sagen SOLLTEN und rot für Dinge, die sie NICHT sagen sollten. Dies ist auch der Zeitpunkt, an dem Sie ein vorläufiges Schreiben zur Benachrichtigung über eine Sicherheitsverletzung verfassen sollten.

Testen und trainieren: Führen Sie einige Probeläufe mit dem Plan durch, sowohl als Tabletop-Übung als auch als Red-Team-Szenario, bei dem ein Team die Rolle des Hackers übernimmt. Tabletop-Übungen sind nützlich für die Schulung von Führungskräften und funktionsübergreifenden Teams, während Red-Team-Übungen hervorragend geeignet sind, um die volle Leistungsfähigkeit Ihres Sicherheitsteams und Ihrer Tools zu testen. Stellen Sie sicher, dass alle Teammitglieder für ihre Rollen angemessen geschult sind.

2. Erkennen und Analysieren

Sicherheitsteams werden von verschiedenen Stellen auf einen Vorfall aufmerksam gemacht, unter anderem:

- Menschen: Benutzer, Systemadministratoren, Netzwerkadministratoren, Sicherheitspersonal, MSSPs und andere Personen in Ihrem Unternehmen, die Anzeichen für einen Sicherheitsvorfall melden
- SIEMs oder andere Sicherheitsprodukte, die Warnungen auf Grundlage der Analyse von Protokolldaten erzeugen
- Software zur Überprüfung der Dateiintegrität, die mithilfe von Hash-Algorithmen erkennt, wenn wichtige Dateien verändert wurden
- Anti-Malware-Programme
- Logs/Protokolle (einschließlich auditbezogener Daten), die systematisch überprüft werden sollten, um anomale und verdächtige Aktivitäten an folgenden Stellen zu entdecken:
  - Benutzer
  - Externer Speicher
  - Echtzeitspeicher
  - Netzwerk- und Endpunktgeräte
  - Betriebssysteme
  - Cloud-Dienste
  - App-Anwendungen
- Dritte wie Kunden, Partner in der Lieferkette, Finanzinstitute oder Strafverfolgungsbehörden
- Im Falle von Ransomware unzugängliche verschlüsselte

Sobald ein Vorfall als schwerwiegend eingestuft wird, gemäß den festgelegten Regeln Ihres Vorfallsreaktionsplans, ist es an der Zeit, Ihr Vorfallsreaktionsteam zusammenzurufen und mit der Vorfallsanalyse zu beginnen.

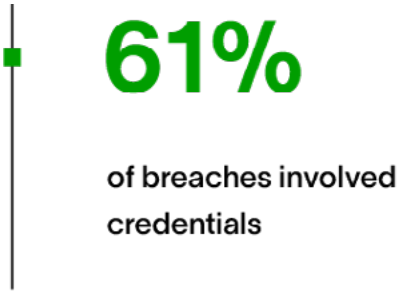


Abbildung 03 Laut dem 2021 Data Breach Investigations Report von Verizon waren an 61 % der Datenschutzverletzungen Zugangsdaten beteiligt. (Bildquelle)

Das Team und seine Sicherheitsanalysten sollten alle zugehörigen Sicherheits-Tools, Protokolle und andere relevante Informationen sammeln und untersuchen und einem vordefinierten Prozess folgen, um den Umfang des Vorfalls zu bestimmen. Dies ist der Zeitpunkt, an dem es äußerst wertvoll ist, Ihr Wissen über normales und abnormales System-, Benutzer- und Netzwerkverhalten einzubeziehen. Nutzen Sie diese Informationen, um:

- Bestimmt den Umfang (Systeme, Netzwerke, Daten und andere IT-Komponenten) der Sicherheitsverletzung
- Die von den Angreifern eingesetzten Techniken, Taktiken und Prozeduren (TTPs) zu verstehen

- Alle damit zusammenhängenden Ereignisse in Beziehung zu setzen (korrelieren) und eine Vorfallszeitachse zu erstellen

Beziehen Sie Bedrohungsdaten und das MITRE(R) ATT&CK-Framework ein, um zusätzlichen Kontext zu sammeln. Dokumentieren Sie die Entscheidungen der Teams und die getroffenen Maßnahmen für die Einhaltung der Vorschriften und künftige Lerneinheiten.

Dies ist auch der richtige Zeitpunkt, um den Rechtsbeistand und die Stakeholder zu informieren. Das werden wir im Abschnitt „Reagieren" ausführlicher behandeln.

3. Eindämmen und beseitigen

Ein Sicherheitsvorfall kann einem Waldbrand ähneln. Die Feuerwehr muss das Feuer unterbinden, um eine Ausbreitung zu verhindern, und es löschen, um den Gesamtschaden zu begrenzen. Ebenso müssen Sicherheitsteams die aktive Bedrohung eindämmen und gleichzeitig daran arbeiten, dem Angreifer die Fähigkeit zu nehmen, dem Unternehmen weiteren Schaden zuzufügen. Während dieser Zeit müssen sie alle Angriffsinformationen und Beweise für zukünftige Analysen aufbewahren.

Zu den Eindämmungsmaßnahmen gehören die Deaktivierung des Netzwerkzugriffs für Computer, die bekanntermaßen mit Malware infiziert sind, die Deaktivierung von Benutzer- und Dienstkonten und die Einschränkung des Zugriffs auf Assets, in denen wichtige Daten und Anwendungen gespeichert sind.

Prozessteams können potenziell bösartige Dateien in einer Sandbox detonieren, um deren Absicht zu verstehen, Sicherheits-Patches zu installieren oder Sicherheits- und andere Tools aufzurüsten. Sie können Passwörter für Benutzer mit kompromittierten Konten zurücksetzen oder Konten von Insidern sperren, die den Vorfall verursacht haben könnten.

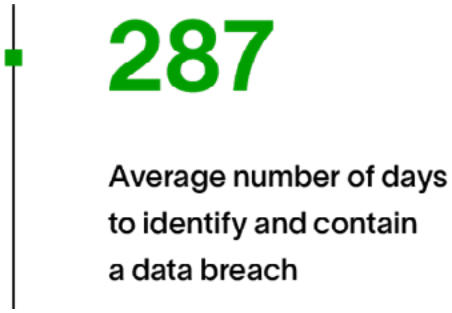


Abbildung 04 Unternehmen benötigen durchschnittlich 287 Tage, um eine Datenschutzverletzung zu erkennen und einzudämmen. (Bildquelle)

Weitere Maßnahmen sind die Durchführung von Schwachstellenanalysen und die Stärkung aller relevanten Zugangspunkte. In dieser Phase stellen Sie fest oder bestätigen, welche Daten gestohlen wurden oder verloren gegangen sind.

Je besser Ihr Plan und Ihre Tools sind, desto wahrscheinlicher ist es, dass Sie nicht unter- oder überreagieren, was beides dazu führen kann, dass eine Sicherheitsverletzung kostspieliger wird als nötig.

Stellen Sie sicher, dass Ihr Team Kopien der infizierten Systeme in einem sicheren, nicht vernetzten Bereich aufbewahrt, um später eine tiefgreifende forensische Analyse zu ermöglichen.

4. Antworten

Wir haben alle relevanten Informationen zur Reaktion in diesen Abschnitt aufgenommen, aber Sie werden wahrscheinlich mit Ihrem Reaktionsprozess beginnen wollen, sobald Sie einen schwerwiegenden Vorfall oder eine Sicherheitsverletzung verifiziert haben, insbesondere wenn es sich um die Offenlegung personenbezogener Daten (PII) von Kunden oder Mitarbeitern handelt.

An dieser Stelle sollte sich Ihr Team mit den Rechtsberatern Ihres Unternehmens zusammensetzen, um die regulatorischen und sonstigen Compliance-Risiken zu verstehen. Die SEC-Bestimmungen für börsennotierte Unternehmen sowie Datenschutzgesetze wie die DSGVO können im Falle einer solchen Datenschutzverletzung eine

rasche öffentliche Bekanntgabe verlangen.

Arbeiten Sie mit Mitgliedern der Rechtsabteilung und des Kommunikationsteams zusammen, um Ihr im Voraus geplantes Benachrichtigungsschreiben zu verfeinern, und verwenden Sie es, um betroffene Kunden und andere Parteien zu benachrichtigen, damit sie sich vor Identitätsdiebstahl oder anderen Folgen der Offenlegung von PII oder Finanzdaten schützen können. Sobald die Kunden benachrichtigt wurden, benötigen Sie wahrscheinlich geschulte Callcenter-Mitarbeiter, um Kundenanfragen effektiv zu beantworten.

Möglicherweise möchten Sie weitere Maßnahmen zum Schutz Ihrer Kunden ergreifen, wie z. B. die Bezahlung eines einjährigen Schutzes vor Identitätsdiebstahl oder eines Kreditüberwachungsdienstes.

Virtuelle oder persönliche Meetings mit Ihren größten Kunden sind zusätzlich notwendig, falls ernsthafte Umsatz- und Reputationsprobleme entstehen.

Stellen Sie sicher, dass klar ist, wer mit den Medien oder der Öffentlichkeit kommunizieren darf (und wer nicht) und was sie sagen können und was nicht. Ausgewiesene Sprecher sollten mit der Öffentlichkeitsarbeit oder der Unternehmenskommunikation zusammenarbeiten, um die interne und externe Reaktion Ihres Unternehmens effektiv zu gestalten.

Stellen Sie sicher, dass das Sicherheitspersonal, die Verantwortlichen für die betroffenen Anwendungen und die Geschäftsleitung an diesen Gesprächen beteiligt sind, um sicherzustellen, dass jeder die genaue Vorgeschichte, den Umfang und die Auswirkungen des Vorfalls oder der Sicherheitsverletzung sowie den Umgang damit versteht.

Üben und verfeinern Sie Ihre im Voraus geplanten grünen Aussagen und vermeiden Sie rote Aussagen.

Alarmieren Sie schließlich die Kontakte bei den Strafverfolgungsbehörden, die Sie bereits etabliert haben, falls Maßnahmen auf Behördenseite ergriffen werden sollen. Die Personalabteilung sollte einbezogen werden, wenn das Unternehmen Maßnahmen in Bezug auf Mitarbeiter oder Auftragnehmer in Erwägung zieht.

Einige Unternehmen möchten möglicherweise Sicherheitsberater, Callcenter oder Dienste zur Unterstützung bei Datenschutzverletzungen unter Vertrag nehmen.

5. Wiederherstellen

Dies ist die Phase, in der Sie sicherstellen, dass der Vorfall behoben ist, die Systeme wieder in Betrieb genommen werden und Maßnahmen zur Vermeidung künftiger Vorfälle getroffen werden.

Führen Sie eine System-/Netzwerkvalidierung und -tests durch, um alle Systeme als funktionsfähig zu zertifizieren und jede Komponente, die kompromittiert wurde, als sowohl funktionsfähig als auch sicher zu rezertifizieren.

Versetzen Sie die Systeme in eine bekanntermaßen saubere Produktionsumgebung zurück, damit Sie keine erneute Infektion oder Kompromittierung riskieren, während Sie gleichzeitig die Benutzerkonten und Hintertüren sperren oder eliminieren, die das Eindringen ermöglicht haben.

Prüfen Sie alle Beweise und verschaffen Sie sich ein tieferes Verständnis für die Ursache des Vorfalls und das Ausmaß des verursachten Schadens. Eine klare Verantwortlichkeit für die Ursachenanalyse (Root Cause Analysis, RCA) ist von entscheidender Bedeutung, da Fehler das Unternehmen anfällig für zukünftige Angriffe machen können. Viele Unternehmen versäumen es, sich angemessen mit RCA zu befassen.

Besprechen Sie die gewonnenen Erkenntnisse mit dem Team, um zu verhindern, dass sich ähnliche Vorfälle wiederholen. Dazu könnte die Ausarbeitung eines besseren Plans für das Patchen von Server-Schwachstellen, die Schulung von Mitarbeitern zur Vermeidung von Phishing-Betrug oder die Einführung fortschrittlicher Technologien zur besseren Überwachung von Insider-Bedrohungen gehören.

Ändern Sie Ihre Sicherheitsrichtlinien und die Schulung Ihrer Mitarbeiter entsprechend. Wenn der Angriff beispielsweise darauf zurückzuführen ist, dass ein Mitarbeiter unwissentlich einen E-Mail-Anhang geöffnet hat, sollten Sie unternehmensweite Richtlinien und Schulungen einführen und/oder bestehende Richtlinien/Schulungen überdenken.

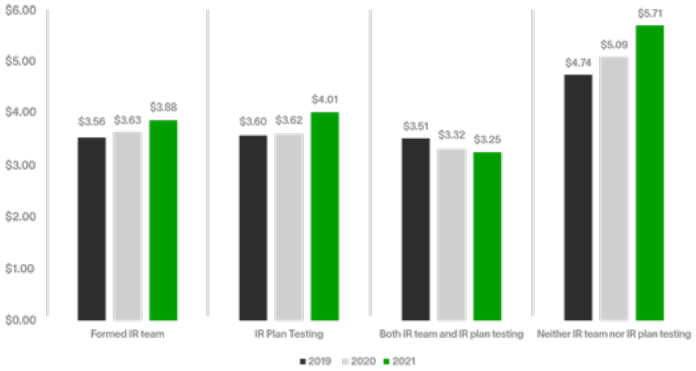
Und schließlich sollten Sie Ihren Vorfallsreaktionsplan aktualisieren, um all diese neuen Präventivmaßnahmen zu berücksichtigen.

Sie brauchen heute und morgen einen Vorfallsreaktionsplan

Ganz gleich, ob Ihr Unternehmen groß oder klein, ein Startup oder ein etabliertes Unternehmen ist, es muss über einen gut getesteten Vorfallsreaktionsplan verfügen, um sicherzustellen, dass es Angriffe schnell und effektiv erkennen, eindämmen und ausmerzen kann, bevor sie erheblichen Schaden anrichten können. Laut dem Cost of a Data Breach Report 2021von IBM und Ponemon konnten allein durch das Vorhandensein eines IR-Teams und das Testen eines IR-Plans die durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2021 um 54,9 % gesenkt werden, gegenüber 42,1 % im Jahr 2020.

Ihr IR-Plan (Vorfallsreaktionsplan) ist eine lebendige Strategie und ein Dokument, das sorgfältig geprüft und auf Grundlage Ihres Unternehmens, der Bedrohungslandschaft und personeller Veränderungen kontinuierlich angepasst werden muss. Das IR-Team sollte sich mindestens einmal im Jahr und nach jedem schwerwiegenden Vorfall treffen, um den Wert des Plans zu beurteilen und sich auf notwendige Änderungen zu einigen.

Jedes Unternehmen wird je nach IT-Umgebung und Geschäftsanforderungen unterschiedliche Verfahren zur Reaktion auf Vorfälle entwickeln. Stellen Sie sicher, dass Ihr Plan immer optimal und effektiv auf die Bedürfnisse Ihres Unternehmens abgestimmt ist.



Über Exabeam

Exabeam ist ein weltweit führendes Unternehmen im Bereich Cybersicherheit, das jeden IT- und Sicherheits-Stack intelligenter macht. Als Marktführer im Bereich der nächsten Generation von SIEM und XDR erfindet Exabeam die Art und Weise neu, wie Sicherheitsteams Analysen und Automatisierung nutzen, um Bedrohungen zu erkennen, zu untersuchen und zu bekämpfen (TDIR), von gewöhnlichen Sicherheitsbedrohungen bis hin zu den kritischsten, die schwer zu erkennen sind. Exabeam bietet eine umfassende, über die Cloud bereitgestellte Lösung, die maschinelles Lernen und Automatisierung mit einem präskriptiven, ergebnisorientierten TDIR-Ansatz nutzt. Wir konzipieren und entwickeln Produkte, die Sicherheitsteams dabei helfen, externe Bedrohungen, kompromittierte Benutzer und böswillige Gegenspieler zu erkennen, Fehlalarme zu minimieren und ihre Unternehmen bestmöglich zu schützen.

exabeam

Weitere Informationen finden Sie unter exabeam.com.