BlackBerry
Intelligent Security. Everywhere.

Solution Brief

Incident Response

Untersuchung, Eindämmung und Behebung von Sicherheitsverletzungen

Herausforderung

Laut einer Analyse von IBM[1] ist „die große Mehrheit" der Unternehmen derzeit nicht darauf vorbereitet, auf einen schweren Sicherheitsvorfall effektiv zu reagieren. Meist ist dies auf anhaltende Ressourcenengpässe und eine unzureichende Planung zurückzuführen.

- Im Jahr 2019 benötigten Unternehmen durchschnittlich 206 Tage, um einen Datenverstoß zu identifizieren und weitere 73 Tage, um ihn einzudämmen. Das entspricht einem Anstieg von fast 5% gegenüber dem Vorjahr.[2]
- Die durchschnittlichen Gesamtkosten eines Datenverstoßes beliefen sich bei Großunternehmen auf 5,11 Millionen Dollar (etwa 204 Dollar pro Mitarbeiter). Bei kleineren Unternehmen lag der Durchschnitt bei 2,65 Millionen Dollar (etwa 3.533 Dollar pro Mitarbeiter). Die höheren proportionalen Kosten für kleinere Firmen können „ihre Fähigkeit zur finanziellen Erholung nach einem Vorfall beeinträchtigen".[3]
- Weniger als ein Viertel der Befragten verfügt über einen Cybersecurity Incident Response Plan (CSIRP), der im gesamten Unternehmen einheitlich angewendet wird. Weitere 49% geben an, dass sie entweder überhaupt kein CSIRP haben oder dass ihr CSIRP informell oder „ad hoc" ist.[4]
- Von den Unternehmen, die über CSIRPs verfügen, versäumt mehr als die Hälfte, diese regelmäßig zu prüfen und zu warten. Der Grund dafür liegt an anhaltender Ressourcenknappheit.[5]

Es gibt keine schnelle Lösung. Der akute weltweite Mangel an erfahrenen Experten im Bereich Cybersecurity wird immer mehr zur Herausforderung. Überlastete und von falschen Alarmen gestresste Sicherheitsmitarbeiter kämpfen darum, Systeme gepatched und auf dem neuesten Stand zu halten. So werden Organisationen anfällig für Angriffe, die ansonsten leicht verhindert werden könnten. Versuche, Lücken durch das Hinzufügen von Sicherheitsebenen zu schließen, können zu einer Sicherheitsinfrastruktur führen, die übermäßig komplex und schwer zu verwalten ist. Unterdessen werden Bedrohungsakteure immer einfallsreicher und entwickeln Taktiken, Techniken und Verfahren (TTPs), die explizit darauf ausgerichtet sind, die auf Signaturen basierenden Abwehrmechanismen zu umgehen, indem sie bösartigen Code verschleiern, Polymorphismus einsetzen oder Dutzende anderer Techniken ausnutzen.

BlackBerry® Security Services kann hier mit Technologien wie künstlicher Intelligenz (K), umfangreichem Expertenwissen und Support unterstützen und damit Organisationen in die Lage versetzen, Sicherheitsverletzungen effizient zu untersuchen, einzudämmen und zu beheben. Sie müssen nicht bereits BlackBerry-Kunde sein, um diesen Support zu erhalten. BlackBerry Security Services stehen für jedes Unternehmen zur Verfügung.

Im Jahr 2019 benötigten Unternehmen durchschnittlich 206 Tage, um einen Datenverstoß zu identifizieren und weitere 73 Tage, um ihn einzudämmen. Das entspricht einem Anstieg von fast 5% gegenüber dem Vorjahr.

Quelle: 2019 Cost of a Data Breach Report IBM Security

1 IBM-Analyse: Über die Hälfte aller Unternehmen mit Cybersecurity Incident Response Plänen versäumt es, diese Pläne zu prüfen
2 2019 Cost of a Data Breach Report IBM Security
3 2019 Cost of a Data Breach Report IBM Security
4 Fourth Annual Study on The Cyber Resilient Organization
5 IBM-Analyse: Über die Hälfte aller Unternehmen mit Cybersecurity Incident Response Plänen versäumt es, diese Pläne zu prüfen

Incident Response von BlackBerry

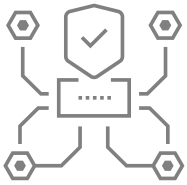
Jeder BlackBerry Security Services Incident Response (IR)-Einsatz durchläuft unter Nutzung der BlackBerry KI-Technologien und unseres Expertenwissens fünf verschiedene Phasen, in denen die BlackBerry-KI-Technologie und das Fachwissen der globalen IR-Teams voll zum Tragen kommen. Diese fünf Phasen laufen gleichzeitig ab, ermöglichen dynamische, schnelle Reaktionen auf sich entwickelnde Zwischenfälle und verkürzen den kritischen Pfad zur Eindämmung.

Während des Kickoff-Meetings stimmen sich die BlackBerry- und Kunden-IR-Teams ab, um den Umfang des Einsatzes festzulegen, die anfänglichen Kompromissindikatoren (IOCs) zu überprüfen und einen Projektplan und einen vorläufigen Zeitplan zu entwickeln. Im Ergebnisprotokoll des Meetings wird Folgendes festgehalten:

- Wie der Angriff ursprünglich entdeckt wurde
- Die erhobenen Daten
- Ein vorläufiges Bedrohungsprofilile
- Bisherige Maßnahmen zur Schadensbegrenzung
- Die Projektprioritäten und -ziele des Auftraggebers

PHASE 1

Bereitstellung:



Wenn ein Zwischenfall eintritt, ist es wichtig, alle IOCs so schnell wie möglich zu identifizieren. Zu Beginn stellt das BlackBerry-IR-Team dem Kunden eine Reihe von Software-Tools zur Erfassung forensischer Daten und zum unternehmensweiten Scannen nach Malware zur Verfügung. Dazu gehören einfache Triage-Skripts und der einheitliche agile Agent für BlackBerry® Protect und BlackBerry® Optics. Der Installations- und Ausführungsprozess des Tools ist für die Anwender transparent, da der Agent nur minimale Systemressourcen verbraucht und die Skripte nur fünf bis fünfzehn Minuten laufen, bevor sie beendet werden.

BlackBerry Protect ist eine herausragende Endpoint Protection Lösung, die mithilfe von KI die Ausführung von Malware mit einer nachgewiesenen Wirksamkeit von 99,1 % verhindert. Bei vielen Einsätzen kann die Aktivierung von BlackBerry Protect im automatischen Quarantänemodus einen laufenden Übergriff sofort stoppen, indem Malware auf infizierten Systemen neutralisiert wird. BlackBerry Protect umfasst auch Sicherheitskontrollen, die skriptbasierte, dateifreie, auf Speichern oder externen Geräten basierende Angriffe vereiteln.

BlackBerry Optics ist eine KI-gesteuerte Endpoint Detection and Response (EDR) Lösung, die erweiterte Funktionen für die Ursachenanalyse, die intelligente Bedrohungssuche und die Initiierung von Playbook-gesteuerten automatisierten Reaktionen bietet, die weit verbreitete Sicherheitsvorfälle verhindern. Durch die Zusammenarbeit von BlackBerry Protect und BlackBerry Optics werden Vorfälle schneller beseitigt und kompromittierte System neutralisiert.

BlackBerry Protect ist eine herausragende Endpoint Protection Lösung, die mithilfe von KI die Ausführung von Malware mit einer nachgewiesenen Wirksamkeit von 99,1 % verhindert.

PHASE 2

Erfassung

Sobald die Bereitstellung abgeschlossen ist, legt das BlackBerry-IR-Team die Rohdaten fest, die es für die Analyse benötigt, und unterstützt den Kunden bei der Erfassung. Dazu gehören typischerweise Dateisystem-Metadaten von Endpunkten, Protokolldaten von Netzwerkgeräten, Ereignis- und Alarmdaten von zusätzlichen Sicherheitssystemen und vieles mehr. Als nächstes setzt das BlackBerry-Team proprietäre Cloud-basierte Tools und Methoden ein, um die Daten zu normalisieren, zu kontextualisieren, anzureichern und zu formatieren. Die so erhaltenen forensischen Artefakte werden mit einer proprietären Analyse-Engine verarbeitet und sicher in der BlackBerry-Cloud für externe Analysen gespeichert.

PHASE 3

Analyse

Während der Analysephase nutzt das BlackBerry-Team:

- BlackBerry Protect zum Erkennen und Beenden von Malware, bösartigen PowerShell-Skripten, Speicherinjektionsangriffen und mehr.
- BlackBerry Optics, um nach Beweisen für Datenexfiltration und Sabotage, Befehls- und Kontrollaktivitäten, Anomalien bei der Benutzerauthentifizierung, Persistenzmechanismen für Malware, anomalen Netzwerk-Host- und Anwendungskonfigurationen und vielem mehr zu suchen.
- Die BlackBerry eigene intelligente Bedrohungsdatenbank zum Durchsuchen von Kundendaten nach bekanntermaßen schlechten IOCs.

Die daraus resultierenden Erkenntnisse werden nach Prioritäten geordnet, dem Kunden mitgeteilt und in detaillierte Aktionspläne für eine effiziente Sanierung und Säuberung aufgenommen.

PHASE 4

Abhilfe

Die IR-Aktionspläne der BlackBerry Security Services legen die Reihenfolge der Schritte fest, die erforderlich sind, um den Verstoß zu beenden und zu verhindern, dass er sich wiederholt. Eine fortgeschrittene persistente Bedrohung (Advanced Persistent Threat, APT) lässt sich beispielsweise nicht einfach durch das Löschen bösartiger Dateien und das Beenden laufender Prozesse lösen. Persistenzmechanismen müssen zuerst deaktiviert werden, wie z.B. geplante Tasks, die bösartigen Code laden, der in der Systemregistrierung versteckt ist. BlackBerry Optics spielt hier eine wesentliche Rolle, indem es automatisierte Playbook-Regelsätze initiiert, um diese Aktionen in der richtigen Reihenfolge auszuführen und Umgebungsdaten zu sammeln. So wird sichergestellt, dass keine Artefakte zurückbleiben. Es können auch allgemeingültige Regeln erstellt werden, um TTPs gemeinsamer Bedrohungsakteure zu vereiteln, wie z.B. der Missbrauch der Windows-Ereignisanzeige (wevutil), um der Erkennung zu entgehen, indem Systemprotokolle gelöscht oder der Protokollierungsdienst abgeschaltet wird.

PHASE 5

Reporting

Zum Abschluss des IR-Engagements erhält der Kunde einen zweiteiligen Bericht. Teil 1 ist eine Zusammenfassung, in der die wichtigsten Ergebnisse in nicht-technischer, für die Verantwortlichen des Unternehmens geeigneter Form dargestellt werden. Teil 2 beschreibt jeden Schritt der Untersuchung und listet die entdeckten Artefakte, die resultierenden IOCs, den ursprünglichen Infektionsvektor, den Umfang und die Ausbreitung des Eindringens, die Auswirkungen auf die Infrastruktur und die Maßnahmen zu deren Neutralisierung auf. Der Bericht schließt mit sowohl taktischen als auch strategischen Empfehlungen, nicht nur zur Verhinderung ähnlicher Angriffe in der Zukunft, sondern auch zur Stärkung der allgemeinen Sicherheitslage des Auftraggebers. Dazu gehören z.B. das Vorschlagen zusätzlicher Mitarbeiterschulungen nach einem Phishing-Angriff, die Durchführung spezifischer Upgrades für anfällige Systeme und das Offline-Nehmen aller externen RDP-Systemzugriffe.

Bereitstellung:

BlackBerry Protect und BlackBerry Optics beschleunigen die Erkennung und Reaktion.

Erfassung

Die Methoden sind effizient, einfach und für das Unternehmen transparent.

Analyse

Versierte IR-Experten identifizieren IOCs schnell und umfassend.

Abhilfe

BlackBerry Optics initiiert automatisch Sanierungs- und Beseitigungspläne.

Reporting

Dokumentiert geschäftliche Auswirkungen, technische Details und bewährte Sicherheitsverfahren.

Vorteile für den Kunden

Der mehrstufige IR-Ansatz der BlackBerry Security Services bietet Kunden direkte Vorteile.

- **Schnelle Erkennung:** Durch die Integration von künstlicher Intelligenz (KI) in ihre Werkzeuge und Prozesse erzielen BlackBerry-IR-Teams schnell vorläufige Ergebnisse. Die Erkennung und Eindämmung von Ransomware und APTs kann innerhalb weniger Stunden nach Abschluss der Datenerfassung beginnen.
- **Schnelle Reaktion:** Die Zeit, die ein traditionelles Beratungsunternehmen benötigt, um die Sicherheitsumgebung eines Kunden zu bewerten oder auf einen potenziellen Verstoß zu reagieren, kann Wochen betragen. Dadurch kann sich der Schaden ausbreiten und die Kosten für die Wiederherstellung und Säuberung gehen in die Höhe. Die IR-Experten der BlackBerry Security Services stehen jederzeit zur Verfügung, um konsistente, erstklassige Dienstleistungen anzubieten.

- **Schnelle Abhilfe:** Sobald BlackBerry Protect im automatischen Quarantänemodus aktiviert ist, wird verhindert, dass Malware auf infizierten Systemen ausgeführt wird und sich lateral über das Netzwerk verbreitet. BlackBerry Optics kann dann eine Sequenz automatisierter Abhilfemaßnahmen einleiten, welche die Bedrohung effizient neutralisieren und zur Bereiningung der vorhandenen Umgebung beitragen.
- **Low-Touch-Datenerfassung:** Die Methoden der Datenerfassung sind effizient und transparent. Es ist zum Beispiel nicht notwendig, Hardware und Geräte auf Host-Systemen oder auf Internet-Ausgangspunkte festzulegen Stattdessen erhält der Kunde BlackBerry Protect und BlackBerry Optics, die auf den Endpunkten mit den vorhandenen Bereitstellungsmethoden installiert werden können. Alternativ können Sie mit schlanken Skripten ausgestattet werden, die auf jedem Endpunkt zwei bis fünf Minuten lang ausgeführt und dann beendet werden, wobei nur minimale Artefakte zurückbleiben.
- **Kosten- und Ressourceneffizienz:** Sofern vom Kunden nicht anders gewünscht, arbeiten die BlackBerry-IR-Teams remote, wodurch Reisekosten und Kosten für Ressourcen vor Ort entfallen.
- **Prävention - erste Verteidigungsschritte:** Nach Abschluss jedes IR-Einsatzes der BlackBerry Security Services haben Sie die Möglichkeit, BlackBerry Protect und BlackBerry Optics Lizenzen für die auf Ihren Endgeräten installierten Software zu erwerben oder den BlackBerry® Guard Managed Detection and Response Service zu abonnieren. In beiden Fällen stehen Ihnen ThreatZero®-Berater zur Verfügung, um Sie in der Übergangsphase zu unterstützen, indem sie die Sicherheitskontrollen von BlackBerry Protect zur Malware-Prävention, zum Schutz vor Speicherausnutzung, zur Durchsetzung von Geräterichtlinien sowie zur Anwendungs- und Skriptkontrolle im vollständigen Blockierungsmodus aktivieren.

Mehr erfahren

Weitere Informationen über die Incident Response- und Forensik-Unterstützung der BlackBerry Security Services erhalten Sie, wenn Sie eine Beratung anfordern oder wenn Sie **+1-888-808-3119** für sofortige Hilfe anrufen.

Über BlackBerry Security Services

Die Beratungseinsätze der BlackBerry Security Services ermöglichen es Kunden, ihre unternehmenskritischen Abläufe zu sichern und ihre Endpunkte, Arbeitsbereiche und Identitäten innerhalb einer Zero Touch, Zero Trust-Architektur zu verwalten. Unsere Berater verfügen über das fundierte Wissen und die investigative Erfahrung, die Organisationen benötigen, um iCyber-Risiken zu minimieren und anhaltende, gut finanzierte Angriffe abzuwehren. Gemeinsam helfen wir unseren Kunden, das gesamte Spektrum der Herausforderungen im Bereich der Cybersicherheit anzugehen und eine starke und effektive Sicherheitsinfrastruktur aufzubauen, indem wir Methoden der Prävention zuerst anwenden. Bitte besuchen Sie unsere Consultingseiten für eine vollständige Liste der BlackBerry Security Services-Lösungen.

Für weitere Informationen besuchen Sie BlackBerry.com und folgen Sie @BlackBerry.

BlackBerry®
Intelligent Security. Everywhere.

MKTG 20-0023 | 201123