BlackBerry
Intelligent Security. Everywhere.

Solution Brief

Compromise Assessment

Identifizierung und Bewertung von bereits erfolgten Datenlecks, um künftige Vorfälle proaktiv zu verhindern

Herausforderung für Unternehmen

Angesichts der Tatsache, dass Cyberangriffe sowohl an Quantität als auch an Raffinesse zunehmen, fragt es sich, wie eine Organisation mit Sicherheit wissen kann, ob sie nicht bereits kompromittiert wurde. Wie leicht lassen sich Art und Umfang eines Datenlecks feststellen? Wie schnell kann eine Sicherheitsverletzung erkannt und behoben werden? Vielen Unternehmen mangelt es heute an der notwendigen Visibilität, an Toolsets, Ressourcen und Erfahrung, um diese Fragen mit Zuversicht beantworten zu können. Die Tendenzen sind beunruhigend. 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.[1]

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 darauf ausgerichtet sind, die auf Signaturen basierenden Abwehrmechanismen zu umgehen, indem sie bösartigen Code verschleiern, Polymorphismus einsetzen oder Dutzende anderer Techniken ausnutzen.

Ein BlackBerry® Security Services Compromise Assessment (CA) kann hier unterstützen und die Unsicherheit verringern, indem Kunden eine umfassende Analyse ihrer Cyber-Risiken zur Verfügung gestellt wird. Zu den Schwerpunktbereichen gehört:

- Ausschleusen und Sabotage von Daten
- Kommando- und Kontrollaktivitäten
- Anomalien bei Benutzerkonten
- Malware und Persistenzmechanismen
- Verwundbare Netzwerk-, Host- und Anwendungskonfigurationen

Wenn Beweise für einen Verstoß in der Vergangenheit entdeckt werden, können die Experten von BlackBerry feststellen, wann, wo und wie er aufgetreten ist, und taktische Empfehlungen zur Verhinderung einer Wiederholung geben. Wenn gegenwärtig ein Verstoß im Gange ist, kann das BlackBerry-Team sofort in den Incident Respons (IR) Modus übergehen, die Kill-Chain zurückverfolgen und die TTPs identifizieren, die der Angreifer verwendet hat, um seine Ziele zu erreichen.

Durch die Integration von künstlicher Intelligenz (KI) in ihre Werkzeuge und Prozesse erzielen die Berater von BlackBerry schnell erste Ergebnisse. Ransomware und Advanced Persistent Threats (APTs) werden oft innerhalb von Stunden nach Abschluss der ersten Datensammlung entdeckt.

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 2019 Cost of a Data Breach Report IBM Security

Compromise Assessment von BlackBerry

Unsere Consultants verwenden eine KI-basierte Best-Practice-Methodik zur Bewertung von Umweltrisiken, zur Identifizierung von Sicherheitsvorfällen und zur Aufdeckung laufender Aktivitäten von Bedrohungsakteuren in einer Netzwerkumgebung. Sämtliche Einsätze des CA-Teams befassen sich mit den Bereichen der Verfolgung nach Bedrohungen und der Reduzierung der Angriffsfläche und reichen von der anfänglichen Beurteilung bis hin zur gezielten Beurteilung.

Phase 1 Anfängliche Beurteilung

In der ersten Beurteilungsphase wird dem Kunden ein einfaches Paket von Software und Skripten zur Erfassung der Daten zur Verfügung gestellt, die das Team für die Verfolgung nach anomalem Verhalten, IOCs und anderen Risiken für die Umgebung benötigt. Dazu gehören typischerweise Dateisystem-Metadaten von Endpunkten, Protokolldaten von Netzwerkgeräten, Event- und Warndaten von zusätzlichen Sicherheitssystemen und mehr. Als Nächstes verwendet das Team proprietäre Cloud-basierte Tools und Methoden, um die Daten zu normalisieren, zu kontextualisieren, anzureichern und zu formatieren. Die sich daraus ergebenden forensischen Artefakte werden mit einem firmeneigenen Analysemodul verarbeitet und vom CA-Team überprüft, um Interessenten und Aktivitäten zu identifizieren, die weitere Untersuchungen erfordern.

Phase 2 Gezielte Beurteilung

In der nächsten Beurteilungsphase werden eigenständig ausführbare Dateien verteilt, um detailliertere forensische Daten über die verdächtige Aktivität zu sammeln, die während der anfänglichen Beurteilung markiert wurde. Wenn ein aktiver Verstoß entdeckt wird, kann das BlackBerry-CA-Team sofort auf den Vorfall reagieren, indem es bewährte IR-Methoden verwendet, um die Kill Chain zu verfolgen, ausgenutzte Schwachstellen zu dokumentieren, Auswirkungen zu bewerten und Abhilfemaßnahmen zu erstellen.

Gelieferte Ergebnisse

Zum Abschluss des Einsatzes legt das BlackBerry-Beratungsteam einen umfassenden Bericht mit seinen Ergebnissen und Empfehlungen vor:

- **Ergebnisse der Bedrohungssuche:** Wurde ein früherer oder aktueller Konflikt festgestellt, werden dessen Art, Ausmaß und Auswirkungen auf die Umgebung detailliert beschrieben.
- **Ergebnisse der Reduzierung der Angriffsfläche:** Strategische und taktische Empfehlungen zur Verbesserung der Sicherheitssituation des Unternehmens werden detailliert aufgeführt, ebenso wie eine risikopriorisierte Bewertung der Möglichkeiten zur Reduzierung der Angriffsfläche.

Es besteht die Möglichkeit zur Planung einer Präsentation mit dem Vorstand sowie den Fachbereichs- und IT-Leitern des Kunden, um die während des Einsatzes aufgeworfenen Sicherheitsfragen zu erörtern und eine sicherheitsbewusstere Kultur zu etablieren.

In der ersten Beurteilungsphase wird dem Kunden ein einfaches Paket von Software und Skripten zur Erfassung der Daten zur Verfügung gestellt, die das Team für die Verfolgung nach anomalem Verhalten, IOCs und anderen Risiken für die Umgebung benötigt.

Vorteile für den Kunden

BlackBerry Security Services CA hilft Unternehmen dabei, einen proaktiven, auf Prävention basierenden Ansatz bei ihrer Sicherheitsstrategie zu verfolgen. Vergangene Sicherheitsverstöße können identifiziert und ihre Ursachen bewertet werden, um eine Wiederholung zu verhindern. Laufende Sicherheitsverstöße können zurückverfolgt, beendet und behoben werden. Das Vertrauen in die Sicherheitslage des Unternehmens wird wieder hergestellt. Zu den typischen Vorteilen gehören:

- **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 CA-Experten der BlackBerry Security Services stehen jederzeit zur Verfügung, um konsistente, erstklassige Dienstleistungen anzubieten.
- **Schnelle Erkennung:** Durch den Einsatz von BlackBerry-KI-Technologie und -Prozessen können BlackBerry-CA-Teams oft innerhalb weniger Stunden nach Beginn der Analyse schnell vorläufige Ergebnisse erzielen.
- **Umfassende Analyse:** Die Tools von BlackBerry unterstützen die netzwerkweite forensische Analyse und nutzen IOCs aus Tausenden von früheren Beratungsmandaten.
- **Low-Touch-Datenerfassung:** Die schlanke BlackBerry Datenerfassungs- und -analysesoftware wird vom Kunden installiert und erfordert nur minimale Systemressourcen für einen effizienten Betrieb. So entfällt für sie die Notwendigkeit, Hardware oder Geräte auf Hostsystemen oder an Internet-Ausgangspunkten bereitzustellen.
- **Möglichkeiten für den Aufbau von Fähigkeiten für interne Sicherheits-Teams:** Die strategischen Malware-, forensischen und Protokollanalyse-Berichte, die von den BlackBerry-CA-Beratern erstellt werden, bieten internen Teams die Möglichkeit zur Weiterbildung und zum Kompetenzaufbau.
- **Kosten- und Ressourceneffizienz:** Sofern vom Kunden nicht anders gewünscht, arbeiten BlackBerry-Teams remote, wodurch Reisekosten und Kosten für dedizierte Ressourcen vor Ort entfallen.
- **Proaktive Risikoreduzierung:** Unternehmen lernen aus vergangenen Sicherheitsverstößen, wie sie Cyberrisiken reduzieren und zukünftige Vorfälle verhindern können.

Mehr erfahren

Für weitere Informationen über BlackBerry Security Services for Incident Response and Containment fordern fordern Sie bitte eine Beratung an oder rufen Sie **+1-888-808-3119** an für sofortige Unterstützung.

BlackBerry Security Services

Die Beratungseinsätze der BlackBerry Security Services ermöglichen es Kunden, ihre unternehmenskritischenSysteme 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, um Cyber-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 auf Methoden der Prävention setzen. 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.

PS20-0416 | 201123