BlackBerry
Intelligent Security. Everywhere.

Whitepaper

Ransomware-Prävention ist möglich

Einführung

Ransomware ist eine bösartige Schadsoftware, die sensible Dateien verschlüsselt, sodass die Eigentümer nicht mehr auf ihre Daten und Systeme zugreifen können. Betroffene können dann die Dateien meist nur über Sicherungskopien oder den Kauf eines Entschlüsselungsschlüssels wiederherstellen. Wer aber nicht schnell genug auf die Erpressung reagiert, spürt schnell die Folgen. In den meisten Fällen erhöhen die Angreifer ihre Forderung oder löschen einfach den dringend benötigten Entschlüsselungsschlüssel.

Die Strafverfolgungsbehörden raten den Opfern generell davon ab, auf die Erpressung einzugehen. Dennoch zahlen viele Unternehmen das Lösegeld. In der trügerischen Hoffnung, eine Störung der Betriebsabläufe, unnötige Folgen für Kunden und Aktionäre, teure Wiederherstellungskosten, empfindliche Bußgelder und große Imageschäden abwenden zu können.

Ransomware ist ein äußert lukratives Geschäft. Nicht nur für kriminelle Organisationen, sondern auch für staatlich geförderte Akteure. Fast 27 %[1] aller Sicherheitsvorfälle gehen allein auf Malware zurück. Das spiegeln auch die Zahlen wider. Die Statistiken und Prognosen sind alles andere als beruhigend:

- Bis Ende 2021[2] wird es alle 11 Sekunden einen Ransomware-Angriff auf Unternehmen geben. Und alle 40 Sekunden wird einer dieser Angriffe gelingen[3].
- 62 % der Unternehmen, die auf den Cyberthreat Defense Report 2020[4] geantwortet haben, waren schon Opfer einer Ransomware-Attacke. Und 58 % von ihnen haben tatsächlich die Forderungen der Erpresser erfüllt. Dies entspricht einem Anstieg von 13 % gegenüber dem Vorjahr.

Ransomware als Cyberwaffe

Die BlackBerry Research and Intelligence Unit identifizierte 2020 wichtige Trends bei den Ransomware-Angriffen. Der BlackBerry 2020 Threat Report zeigt deutlich, wie gezielt die Angreifer vorgehen und wie punktgenau sie Ransomware einsetzen, z. B. die Ransomware-Familien Sodinokibi, Ryuk und Zeppelin[5].

Der globale WannaCry-Angriff[6] traf 2017 namhafte Ziele und richtete weltweit immensen Schaden an. Nach einer ruhigeren Phase kehrte Ransomware mit voller Wucht zurück. Ransomware-Angriffe waren bis dahin eine Spezialität von finanziell motivierten Kriminellen. Ihre Opfer waren einzelne Anwender sowie kleine und mittelständische Unternehmen. In jüngster Zeit hingegen sind zunehmend große Unternehmen, öffentliche Einrichtungen und Regierungen im Visier der Angreifer.

Bei hochgesicherten IT-Umgebungen wählen die Angreifer ihre Opfer besonders sorgfältig aus. Sie führen gründliche Erkundungen durch, um den besten Weg ins Innere zu finden. Haben sie sich erst einmal Zugang zur Umgebung des Opfers verschafft, nutzen sie Malware zum Datendiebstahl.

---

1 Verizon 2020 Data Breach Investigations Report
2 Die globalen Kosten für Ransomware-Schäden erreichen bis 2021 voraussichtlich einen Wert von 20 Milliarden US-Dollar
3 What It Means To Have A Culture Of Cybersecurity
4 2020 Cyberthreat Defense Report
5 BlackBerry 2020 Threat Report
6 WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017

Sie transferieren sensible Daten und verschlüsseln sie dann[7]. Wer die Lösegeldzahlungen verweigert, dem drohen die Angreifer mit der Veröffentlichung der gestohlenen Informationen. Handelt es sich dabei um persönliche Kundendaten oder sensible Unternehmensinformationen, kann dies auch noch eine Datenschutzverletzung darstellen und damit hohe Bußgelder nach sich ziehen. Diese Taktik[8] nutzen rund 10 % der Angriffe, die von den BlackBerry® Sicherheitsprodukten und -services erkannt oder abgewehrt wurden. Ein aktuelles Beispiel hierfür ist die Ransomware-Gruppe Maze[9].

Die häufigste Angriffsform ist allerdings nach wie vor das Phishing. Doch auch TTPs (Taktiken, Techniken und Prozeduren) werden immer beliebter. Hierbei muss niemand mehr auf einen bösartigen Link klicken oder ein kompromittiertes Dokument öffnen. Das BlackBerry® Security Services Incident Response Team hat zudem mehrere Fälle aufgedeckt, bei denen VPNs mit veralteter Software im Einsatz waren. Auch dateilose Exploits wie Cobalt Strike wurden gefunden. Sie übernehmen die Kontrolle über ein unsicheres System, indem sie die Prozesse attackieren und bösartigen Code einschleusen. Mithilfe solcher speicherbasierten Angriffe können herkömmliche Antivirenprogramme leicht überwunden werden. Denn diese vertrauen auf den Abgleich von Dateisignaturen und heuristische Techniken zum Schutz der Endpunkte.

Ist der Angreifer erst einmal so weit gekommen, kann er einen alternativen Zugang, eine Backdoor, zu einem Command-and-Control Server (C2) aufbauen. Dies ermöglicht ihm, die Systemregistrierung zu modifizieren, die Persistenz aufrechtzuerhalten und bösartige Tools zu laden. So kann er in Ruhe das Netzwerk erkunden, privilegierte Anmeldeinformationen abfangen und Lateral-Movement-Angriffe starten. Erst nach der Identifizierung und Kompromittierung aller interessanten Ziele kommt die Ransomware zum Einsatz.

Bei gezielten Ransomware-Attacken tauchen immer wieder die gleichen Malware-Familien auf. Sie stammen aus dubiosen Untergrundforen und von Ransomware-as-a-Service (RaaS)-Anbietern. Doch nicht immer geht es um Lösegeld. Einige Ransomware-Angriffe sind darauf aus, Prozesse und Dienste gezielt zu stören. Sie vernichten wichtige Daten, fehlerhafte Zahlungsinfrastrukturen und Verschlüsselungsroutinen. Die Entschlüsselung von Dateien und Lösegeldzahlungen werden so unmöglich gemacht.

Anatomie ausgefeilter Ransomware-Angriffe

Ryuk wurde erstmals im August 2018[10] entdeckt und wird mit einer berüchtigten Gruppe von russischen Cyberkriminellen in Verbindung gebracht. Nach FBI-Angaben[11] hat diese zwischen Februar 2018 und Oktober 2019 mehr als 61 Millionen US-Dollar in Bitcoin erpresst[12].

Das National Cyber Security Centre (NCSC) hat Ryuk in seinem Lagebericht vom Juni 2019 als globale Bedrohung eingestuft[13]. Die Autoren haben herausgefunden, dass die Gruppe nach dem ersten Zugriff oft Tage und Monate damit verbringt, das Netzwerk zu erkunden, bevor Ryuk installiert und eingesetzt wird.

---

7 Another ransomware strain is now stealing data before encrypting it
8 Threat Bulletin: Ransomware 2020 – State of Play
9 Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up
10 CISA Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector
11 Ransomware victims are paying out millions a month. One particular version has cost them the most
12 RSA Presentation: Feds Fighting Ransomware: How the FBI Investigates and How You Can Help
13 Ryuk ransomware targeting organisations globally

Der Angriff wurde zuerst von der Technologie-Website Bleeping Computer[14] am 28. September 2020 gemeldet. Bereits fünf Stunden nach der ersten Infektion hatten hunderte Gesundheitseinrichtungen des Unternehmens in den USA keinen Zugang mehr zu ihren Computer- und Telefonsystemen. In der Folge mussten die UHS-Mitarbeiter massenhaft Patiententermine verschieben und Patienten aus der Notaufnahme in andere Einrichtungen umleiten[15].

So konstruierten die Analysten des DFIR-Reports[16] die Kill Chain:

1. Der Zugang gelang über einen Phishing-Angriff, der die BazarLoader-Malware auf dem Computer des Opfers installierte. Bazar ist ein Trojaner, der von der TrickBot-Gruppe[17] entwickelt wurde und neben Code-Signatur-Zertifikaten auch zahlreiche Verschleierungstechniken einsetzt, um nicht entdeckt zu werden[18].
2. Gleich nach der Installation begann Bazar damit, eine Backdoor zum C2-Server des Angreifers aufzubauen und das UHS-Netzwerk mithilfe von Windows-Dienstprogrammen wie Nltest[19] abzubilden. Dies ist ein legitimes Kommandozeilentool für Windows Server, das Listen von Domainservern erstellen kann.
3. Als Nächstes lokalisierten die Angreifer dann den primären Domainserver, um sich mithilfe der Zerologon genannten Sicherheitslücke Administratorrechte zu verschaffen. Diese Schwachstelle wurde in verschiedenen Windows-Server-Versionen gefunden und gilt als brisant. Im Common Vulnerability Scoring System[20] wird Zerologon sogar mit der höchstmöglichen Punktzahl 10,0 aufgeführt.
4. Danach nutzten die Angreifer SMB-Protokolle (Server Message Block) und WMI (Window Management Instrumentation), um das Cobalt Strike-Toolkit einzusetzen. Damit konnten sie dann auch den sekundären Domaincontroller lokalisieren, um dann zum Lateral Movement überzugehen und die Domainerkennung mit PowerShell Active Directory-Skripten fortzusetzen.
5. Nach der Identifizierung von Zielen für den Domainserver und den Datenspeicher, nutzten die Angreifer dieselben Techniken, um die Kontrolle über den sekundären Domainserver zu erlangen.
6. Erst nach der gründlichen Netzwerkerkundung und Zielerfassung nutzten die Angreifer RDP (Remote Desktop Protocol), um Ryuk auf dem primären DNS-Server, den Netzwerkspeichergeräten und den Geräten der Mitarbeiter zu installieren und auszuführen.

---

14 UHS hospitals hit by reported country-wide Ryuk ransomware attack
15 A Ransomware Attack Has Struck a Major US Hospital Chain
16 Ryuk in 5 Hours
17 BazarBackdoor: TrickBot gang's new stealthy network-hacking malware
18 Front Door" into BazarBackdoor: Stealthy Cybercrime Weapon
19 Microsoft command line reference
20 NIST National Vulnerability Database CVE-2020-1472 Detail

Was sollten sicherheitsbewusste Unternehmen tun?

Zunächst einmal ist es wichtig zu wissen, was sicherheitsbewusste Unternehmen nicht tun sollten: Nämlich weitere Sicherheitsebenen einer bereits komplexen und kaum zu überschauenden Sicherheitsinfrastruktur hinzuzufügen. Denn ein Übermaß an Sicherheitskontrollen hat den gegenteiligen Effekt. Die Cyberresilienz nimmt ab statt zu. Laut IBM Security[21] haben fast 30 % der befragten Unternehmen 50 oder mehr Sicherheitstools im Einsatz. Sie schnitten im Vergleich mit Unternehmen, die weniger Tools nutzen, bei der Threat-Erkennung um 8 % und bei der Incident Response (IR) auf Vorfälle um 7 % schlechter ab.

Dies liegt zum Teil an den vielen unnötigen Warnungen, zum Teil aber auch an den riesigen Mengen an Telemetrie- und Ereignisdaten, die von Endpunkten und anderen vernetzten Geräten erzeugt werden. Wie soll ein Analyst solche Datenmengen effizient durchforsten, um das subtile Signal einer Bedrohung aus dem zufälligen Rauschen der Warnungen zu erkennen?

Deshalb sollten Sie erst dann weiter in Cybersicherheit investieren, wenn Ihre Geschäfts- und Sicherheitsleitungsteams ein grundlegendes Verständnis der Cyberrisiken und ihrer eigenen Risikotoleranz haben.

Beginnen Sie mit der Planung und Bewertung

Als erste Maßnahme empfehlen BlackBerry Experten ein Compromise Assessment (CA). Dies hilft Ihnen dabei, die Risikofaktoren zu identifizieren und eine Basis für die Bewertung zukünftiger Sicherheitsupgrades zu schaffen. Das CA sollte unbedingt die Bedrohungssuche und Präventionsfragen näher beleuchten. Es hat sich bewährt, den Fokus auf folgende Aspekte zu legen:

- Datenexfiltration und Sabotage
- Befehls- und Steuerungsaktivitäten
- Anomalien von Benutzerkonten
- Malware und Persistenzmechanismen
- Anfällige Netzwerk-, Host- und Anwendungskonfigurationen

Nehmen Sie Ihre Sicherheits- und Geschäftsleitungsteams mit ins Boot und besprechen Sie mit ihnen das Ergebnis des CAs.

- **Ergebnisse der Bedrohungssuche:** Wenn eine frühere oder aktuelle Kompromittierung festgestellt wird, sollten Sie Art, Umfang und Auswirkungen auf die Umgebung detailliert beschreiben.
- **Erkenntnisse zur Prävention:** Halten Sie in Ihrem Bericht sowohl strategische als auch taktische Empfehlungen zur Verbesserung der allgemeinen Sicherheitslage fest. Auch eine Liste mit den Möglichkeiten zur Reduzierung der Angriffsfläche mit Risikobewertungen ist empfehlenswert. Zudem sollte das CA kritische Schwachstellen wie Zerologon finden und eine Schritt-für-Schritt-Anleitung zur Behebung bereitstellen.

21 Cyber Resilient Organization Report 2020

Laut IBM[22] sind Unternehmen mehrheitlich nicht darauf vorbereitet, angemessen auf einen schweren Sicherheitsvorfall zu reagieren. In einer Umfrage aus dem Jahr 2020[23] stellte IBM fest, dass durchschnittlich 315 Tage vergehen, bis Unternehmen eine Datenschutzverletzung erkennen und beheben. Die Reaktionszeit ist der entscheidende Faktor bei den Folgekosten. Unternehmen, die Vorfälle in weniger als 200 Tagen eindämmen, geben 1,12 Millionen US-Dollar[24] weniger aus als Unternehmen, die länger brauchen.

Deshalb sollten Sie die Fähigkeiten Ihres Abwehrteams zur Identifizierung, Eindämmung, Beseitigung und Wiederherstellung eines Sicherheitsverstoßes formell bewerten. Dazu gehört eine Mitarbeiterbefragung, eine Schwachstellenanalyse der Sicherheitsrichtlinien und eine Bewertung der Leistung des Defensivteams bei einer unternehmensspezifischen IR-Übung. Auf Grundlage dieser Erkenntnisse sollten Sie dann Ihren IR-Plan überarbeiten, um sicherzustellen, dass er die Best Practices der Branche berücksichtigt und den gesetzlichen Standards entspricht.

Solche Assessments sind wichtig, aber sie sind kein Ersatz für Übungen in einem authentischen, realen Angriffsszenario. BlackBerry Security Services bietet Ihnen neben Einbruchs- auch Angreifer-Simulationen an, um Ihren individuellen Sicherheitsanforderungen gerecht zu werden. Einbruchssimulationen sind ideal für Sie, wenn Sie Ihre Verteidigungsfähigkeiten trainieren, Ihre Sicherheitsannahmen überprüfen und Sicherheitslücken identifizieren möchten. Angreifer-Simulationen hingegeben bieten sich an, um die eigenen Fähigkeiten zu trainieren, die es für die Erkennung und Abwehr von gezielten Angriffen braucht.

Weitere Informationen über das Portfolio der BlackBerry Security Services finden Sie auf unserer Website.

BlackBerry Protect verhindert Ransomware-Vorfälle

Angreifer suchen gezielt nach Schwachstellen im System ihrer Opfer, um Ransomware zu hinterlegen. Sei es mithilfe eines bösartigen Skripts oder Malware. BlackBerry® Protect verhindert einen solchen Ransomware-Vorfall effizient. Denn diese Endpoint Protection Platform (EPP)-Lösung vereitelt Cyberangriffe bereits im Vorfeld – dank hochentwickelter künstlicher Intelligenz (KI) und maschinellem Lernen (ML).

Mithilfe der BlackBerry Unified Agile Agent-Technologie wird BlackBerry Protect direkt auf dem Endpunkt eingesetzt. In Millisekunden ist dann klar, ob eine Datei sicher ausgeführt werden kann oder nicht. Spricht nichts dagegen, wird die Ausführung erlaubt, andernfalls wird sie verhindert. In einem solchen Fall wird die Datei direkt unter Quarantäne gestellt. Gleichzeitig zeigt die BlackBerry® Cyber Suite Managementkonsole zahlreiche Warn- und Kontextdaten an. Dieser Prozess läuft unabhängig auf jedem Endpunkt und verbraucht nur minimale Systemressourcen. Es braucht dazu weder eine Remote-Datenbank, ständige Updates noch eine Verbindung zur Cloud. Die BlackBerry Protect KI-Modelle erkennen und verhindern die Ausführung von Malware und Ransomware in offenen und auch in isolierten Netzwerken.

22 IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them
23 IBM Security Cost of a Data Breach Report 2020
24 IBM Security Cost of a Data Breach Report 2020

BlackBerry Protect löst gleich zwei Probleme auf einmal. Es verhindert die Ausführung bösartiger Dateien ebenso wie das Einschleusen von bösartigem Code in den Systemspeicher. Dazu werden alle laufenden 32- und 64-Bit-Prozesse auf Verhaltensweisen überwacht, die mit gängigen Exploits in Verbindung stehen. Wird eine Speicherverletzung erkannt, unterbricht BlackBerry Protect die angestoßene Funktion. So lassen sich Korrekturmaßnahmen ergreifen, bevor Schaden entsteht. Das Spektrum reicht vom Ignorieren des Vorgangs über das Zulassen der Ausführung bis hin zum vollständigen Beenden des Prozesses. So werden Angreifer daran gehindert, Malware – wie beispielsweise Bazar – einzusetzen, um legitime Systemdienste zu kapern.

BlackBerry Protect verhindert auch die Ausführung bösartiger PowerShell-, Active Scripts und Microsoft Office Makro-Skripte im Vorfeld. Diese kamen beispielsweise bei der Attacke auf die UHS zum Einsatz. Denn bedauerlicherweise sind Richtlinien zur Skriptkontrolle meist nur auf den Warnmodus eingestellt, damit Administratoren feststellen können, wer welche Skripte verwendet und unter welchen Bedingungen die Ausführung erlaubt ist. Erst nach Abschluss der Bestandsaufnahme kann der Blockmodus aktiviert werden, der die Ausführung aller Skripte verhindert. Allerdings gilt das nicht für Skripte, die in bestimmten Ordnern installiert sind oder für die explizite Ausschlussregeln gelten.

Die BlackBerry Protect Device Control-Richtlinien minimieren das Risiko, dass einer Ihrer Mitarbeiter Ransomware über ein kompromittiertes Massenspeichergerät in Ihr Netzwerk eingeschleust. Sie verhindern zuverlässig, dass nicht-autorisierte Software installiert, Daten exfiltriert oder Unternehmenssysteme versehentlich gefährdet werden. Dies gilt allerdings nur für Massenspeichergeräte und nicht für Peripheriegeräte, wie z. B. Mäuse und Tastaturen.

BlackBerry Protect Application Control sorgt für den kontinuierlich einwandfreien Zustand der Geräte mit festen Funktionen. Es hindert Angreifer zuverlässig daran, Malware zu installieren, das Betriebssystem, die Firmware, den Netzwerkstack und unterstützende Anwendungen zu verändern.

Mit BlackBerry Optics Ransomware-Bedrohungen identifizieren, beseitigen und bereinigen

Sie wissen bereits: BlackBerry Protect wehrt Ransomware-Angriffe effektiv ab. Wozu brauchen Sie dann noch eine Endpoint Detection and Response (EDR)-Lösung wie BlackBerry® Optics?

Der Unterschied zwischen einer zu 100 Prozent wirksamen Lösung und den über 99 Prozent[25] von BlackBerry Protect ist zwar klein, aber fein. Denn wenn eine Ransomware die erste Verteidigungslinie erst einmal durchbrochen hat, ist es klug, ein System in der Hinterhand zu haben, das den Angriff zuverlässig eindämmt und die Ursachensuche erleichtert.

Ein weiterer Grund ist die sich ständig ändernde Bedrohungslandschaft. Verizon analysierte in seinem 2020 Data Breach Investigations Report[26] die Taktiken der Angreifer und kam zu der Erkenntnis, dass „der prozentuale Anteil von Malware an den Sicherheitsverletzungen in den letzten fünf Jahren stetig gesunken ist“.

25 NSS Labs Advanced Endpoint Protection Cylance Security Value Map, April 2018
26 2020 Data Breach Investigations Report

Hier die genauen Zahlen: „45 % der Angriffe gingen auf Hacking-Attacken zurück, 22 % kamen durch Fehler zustande, 22 % erfolgten durch Social-Engineering-Angriffe und nur 17 % wurden von Malware verursacht." Auf den ersten Blick scheint es, dass Malware als Angriffsmethode an Bedeutung verliert. Tatsächlich zeigt es aber, dass die Angreifer – zumindest in den Anfangsphasen der Kill Chain – vermehrt TTPs einsetzen, die keine portablen ausführbaren Dateien erfordern.

Deshalb ist es sinnvoll, mit BlackBerry Optics die Bedrohungsprävention von BlackBerry Protect zu erweitern. Und zwar durch echte KI-Vorfallprävention, Ursachenanalyse, intelligente Bedrohungssuche sowie automatische Erkennungs- und Reaktionsmaßnahmen. Zudem erfordert BlackBerry Optics – im Gegensatz zu herkömmlichen EDR-Produkten – keine teuren Investitionen in eine lokale Infrastruktur oder reaktive Ansätze, die auf einem kontinuierlichen Daten-Streaming in die Cloud beruhen. BlackBerry Optics wendet stattdessen die Erkennungs- und Reaktionslogik direkt am Endpunkt an. Dies eliminiert die Reaktionslatenz, die den entscheidenden Unterschied zwischen einem kleinen Ereignis und einem großen unkontrollierten Sicherheitsvorfall ausmacht.

Dank der integrierten Context Analysis Engine (CAE) kann BlackBerry Optics die Endpunkte nahezu in Echtzeit überwachen und zuverlässig bösartige oder verdächtige Aktivitäten identifizieren. Die CAE überzeugt durch die eigens von BlackBerry kuratierte und vorgefertigte Erkennungslogik, die zahlreiche abgestufte Reaktionen auslösen kann. Sie basiert auf Erkenntnissen, die das BlackBerry IR-Team vor Ort bei der Eindämmung und Behebung realer Angriffe gesammelt hat. Und auf Regeln, die von BlackBerry Threat Researchern nach der Dekonstruktion und Dokumentation raffinierter Angriffe erstellt wurden. Ein Beispiel hierfür sind die benutzerdefinierten BlackBerry Optics Regeln, die gezielt die von Ryuk-Malware-Varianten[27] verwendeten Techniken markieren und abschwächen.

Erkennungsregeln sind zwar wichtig, können aber nicht jedes Angriffsverhalten abbilden. Deshalb hat das BlackBerry Data Science Team auch Module zur Bedrohungserkennung entwickelt, die auf maschinellem Lernen basieren und bei BlackBerry Optics zum Einsatz kommen. Diese analysieren kontinuierlich die Aktivitäten der Endpunkte, um Zero-Day-, APT- und Living-off-the-Land-Angriffe zu erkennen, wie sie von den modernsten Ransomware-Familien durchgeführt werden.

Darüber hinaus bietet Ihnen BlackBerry Optics neben On-Demand-Maßnahmen auch automatische Reaktionen für den Fall, dass eine CAE-Regel ausgelöst wird oder das maschinelle Lernen ein Problem erkennt. Das Spektrum reicht vom Sammeln forensischer Daten, über eine Systemabschaltung bis hin zu Maßnahmen zur Analyse und Behebung des Vorfalls.

Wird ein Vorfall erkannt, muss er im Detail untersucht werden. Nur so stellen Sie sicher, dass alle Stufen der Kill Chain verstanden und bei den anschließenden Maßnahmen berücksichtigt werden. BlackBerry Optics bietet Ihnen manuelle und automatisierte Tools, damit Sie effizient nach Bedrohungen suchen und eine Ursachenanalyse durchführen können.

---

27 Ryuk Malware Optics Rules

Darüber hinaus vereinfacht BlackBerry Optics auch die Bedrohungssuche. Denn es ermöglicht Ihnen, forensisch relevante Daten über die InstaQuery-Suche (IQ) zu sammeln. IQ ist ein leichtgewichtiges Tool, mit dem Sie Daten von jedem Endpunkt sammeln, die Ergebnisse aggregieren und in einem kontextbezogenen oder intuitiv auswertbaren Format präsentieren können.

Erst kürzlich nutzten die BlackBerry Berater IQ bei einem Ransomware-Angriff auf ein großes Unternehmen. Innerhalb weniger Sekunden war klar, dass es sich bei dem primären Gefährdungsindikator (IOC) um eine Dateierweiterung einer Ransomware handelte, die nur in den USA vorkam. Somit musste niemand Zeit damit vergeuden, die Unternehmungsumgebungen in Europa, Asien und im Südpazifik zu betrachten. Die BlackBerry Berater unterstützten den Kunden außerdem bei vorbeugenden Maßnahmen, um zukünftige Infektionen zu verhindern. Sie erstellten und verteilten benutzerdefinierte Regeln, um dafür zu sorgen, dass die Ransomware sofort erkannt und umgehend unter Quarantäne gestellt wird.

Ransomware-Vorfälle mit dem BlackBerry Ansatz verhindern

Mit den Software- und Servicelösungen von BlackBerry können Sie:

- Ransomware blockieren. Und zwar vor der Ausführung, vor der Ausnutzung legitimer Systemdienste, vor der Einnistung und vor Lateral Movement.
- Ransomware daran hindern, Schaden anzurichten. Denn automatisierte Erkennungs-, Reaktions- und Sanierungs-Maßnahmen helfen Ihnen bei der proaktiven Suche nach Bedrohungen und der Ursachenanalyse.
- die Reaktion auf Ransomware-Vorfälle beschleunigen. Bei anderen Anbietern und Beratern können Wochen vergehen, bis eine Reaktion erfolgt. Mit schlimmen Folgen: Der Schaden wird größer und die Kosten für die Wiederherstellung und Bereinigung der Umgebung steigen rasant. Die Experten von BlackBerry hingegen stehen Ihnen sofort zur Seite und bieten Ihnen effiziente und erstklassige Services.
- Ihr Risiko minimieren. Denn Sie erhalten fachkundige Anleitung und Unterstützung, die Sie für Ihre Cybersicherheit benötigen. So können Sie Lücken in Ihrer Sicherheitsstruktur identifizieren und schließen, Ihre Cyberresilienz stärken, robuste IR-Prozesse implementieren und effizient für präventive Sicherheit sorgen.

Ein paar Gedanken zum Schluss

Ist es also möglich, Ransomware-Vorfälle proaktiv zu verhindern? Die Antwort darauf hängt stark davon ab, was Sie unter Prävention verstehen. Wenn Sie sich einen magischen Schalter wünschen, den Sie nur umlegen müssen, um die Ransomware-Angriffe auszuschalten, dann müssen wir Sie leider enttäuschen. Ohne Engagement geht es nicht. Mit BlackBerry können Sie fast alle Ransomware-Angriffe bereits in der Auslieferungsphase der Kill Chain stoppen, wenn Sie zuvor praktische Schritte zur Abwehr unternommen haben.

Das beginnt mit einer gründlichen Analyse und Bewertung der Infrastruktur. So können Sie Cyberrisiken identifizieren und priorisieren. Spielen Sie Patches immer zeitnah auf, um bekannte Schwachstellen zu eliminieren und eine Ausnutzung zu verhindern. Das Gleiche gilt für Fehler in der Systemkonfiguration. Deaktivieren Sie beispielsweise den externen Zugriff auf RDP-Systeme, um BlueKeep-Exploits zu verhindern[28].

Nehmen Sie sich weiterhin der grundlegenden Sicherheitsmaßnahmen wie Blockieren an. Schulen Sie Ihre Mitarbeiter kontinuierlich, um Social-Engineering-Angriffe abzuwehren. Ersetzen Sie ungenügende Passwortrichtlinien durch die Implementierung von Multi-Faktor-Technologien und kontinuierlichen Authentifizierungslösungen. Führen Sie auch kontinuierliche Sicherheitsbewertungen ein, um die Cyberrisiken durch neue Bedrohungen und digitale Transformationsprojekte zu ermitteln. Dieses Engagement ist zwar eine langfristige Verpflichtung, bringt Ihnen aber auch langfristige und nachhaltige Vorteile.

Mit einigen wenigen Maßnahmen können Sie schnell wichtige Erfolge erzielen. BlackBerry Protect beispielsweise erkennt und stoppt nicht nur Ransomware, sondern verhindert auch, dass dateilose Techniken Fuß fassen können. Einen echten Unterschied macht der Einsatz von KI und maschinellem Lernen, wenn es darum geht, raffinierte Angriffe zu stoppen. Und sollte ein Angriff doch einmal durch Ihre Abwehr schlüpfen, greift BlackBerry Optics ein und löst automatische Reaktions- und Sanierungs-Maßnahmen aus, damit aus einem einfachen Sicherheitsverstoß kein schwerwiegender Sicherheitsvorfall wird.

Die Antwort lautet also: Ja. Ransomware-Prävention ist nicht nur theoretisch möglich, sondern auch praktisch.

Erfahren Sie mehr über das BlackBerry Portfolio an Lösungen zur Prävention und Beseitigung von Ransomware.

Weitere Informationen und Ressourcen von BlackBerry zur Bekämpfung von Ransomware finden Sie auf unserer Website.

28 NIST Vulnerability Database CVE-2019-0708

Über BlackBerry

BlackBerry (NYSE: BB; TSX: BB) bietet intelligente Sicherheitssoftware und -dienste für Unternehmen und Regierungen weltweit. Das Unternehmen sichert mehr als 500 Millionen Endpunkte ab, darunter 175 Millionen Autos, die heute auf unseren Straßen unterwegs sind. Das Unternehmen mit Sitz in Waterloo, Ontario, setzt KI und maschinelles Lernen ein, um innovative Lösungen in den Bereichen Cybersicherheit, Sicherheit und Datenschutz zu liefern, und ist in den Bereichen Endpunkt-Sicherheitsmanagement, Verschlüsselung und eingebettete Systeme führend. Die Vision von BlackBerry ist klar – das Sichern einer vernetzten Zukunft, der Sie vertrauen können.

Besuchen Sie für weitere Informationen BlackBerry.com und folgen Sie @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

MKTG 19-0108 | 210407