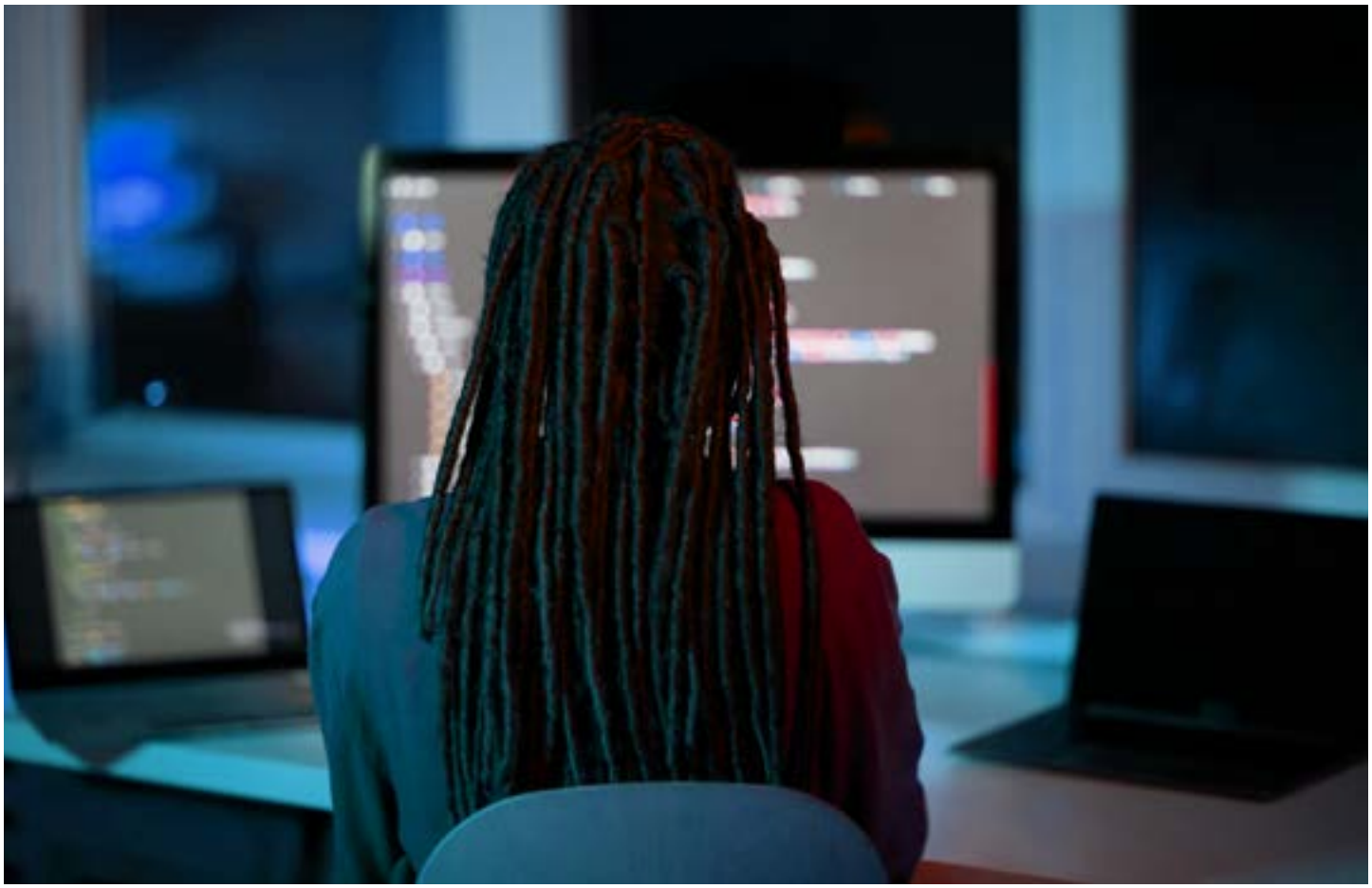
BlackBerry
Intelligent Security. Everywhere.

Business Brief



BlackBerry schützt Sie vor HAFNIUM-Angriffen

Am 2. März 2021 ging Microsoft mit der Nachricht an die Öffentlichkeit[1], dass „mehrere [Zero Day] Exploits entdeckt wurden, die für Angriffe auf lokale Versionen von Microsoft Exchange Server verwendet werden“. Parallel dazu veröffentlichte das Unternehmen mehrere Sicherheitsupdates mit dem dringenden Rat, diese sofort zu installieren. Laut Microsoft gehen die Attacken mit „hoher Wahrscheinlichkeit“ auf das Konto der staatlich geförderten HAFNIUM-Gruppe[2]. In einem Update meldete Microsoft am 5. März eine „verstärkte Nutzung dieser Schwachstellen bei Angriffen auf ungepatchte Systeme auch unabhängig von der HAFNIUM-Gruppe“. Zur Schadensbegrenzung veröffentlichte Microsoft weitere Tools und richtete ein „On-Premises Exchange Server Vulnerabilities Resource Center“[3] ein. Dies bietet seinen Kunden aktuellen HAFNIUM-Support. Berichten und Schätzungen[4] zufolge könnten mindestens 30.000 Microsoft® Exchange Server betroffen sein.

Nach der Analyse der Cyber Kill Chain rät das BlackBerry Threat Research Team[5] allen Exchange Server-Kunden dringend zur Installation der von Microsoft empfohlenen Updates auf allen gefährdeten Systemen.

Die gute Nachricht für BlackBerry Kunden: Die BlackBerry® Cyber Suite Software und die Managed Detection and Response (MDR)-Lösung minimieren die Risiken, die von einer Ausnutzung der Patch-Schwachstellen ausgehen.

- **BlackBerry® Protect** ist eine KI-gesteuerte Endpoint Protection-Lösung. Sie stoppt durch Skriptsteuerung PowerShell-Befehle, die bei HAFNIUM-Angriffen verwendet werden. Darüber hinaus bietet sie Ihnen Speicherschutzfunktionen, die LSASS-Speicherdumps verhindern. Das Speicherextraktionstool der Angreifer wird gestoppt, bevor es die Verarbeitung der Daten abschließen kann.

- **BlackBerry® Optics** ist eine bewährte Endpoint Detection and Response (EDR)-Lösung. Sie reduziert die Auswirkungen der HAFNIUM-Angriffe auf Ihre Unternehmensumgebung. Um den Schutz zu optimieren, rät Ihnen BlackBerry dringend zur Aktivierung der folgenden BlackBerry Optics-Regeln:

  - PowerShell Download
  - Fileless PowerShell Malware
  - PowerShell Encoded Command
  - Hidden PowerShell Execution

  Zudem hat BlackBerry eine aktuelle BlackBerry Optics MITRE-Regel erstellt: Win Procdump Lsass CredTheft. Sie identifiziert die von HAFNIUM verwendeten Techniken und schwächt sie ab. Als BlackBerry Kunde können Sie die Regel herunterladen. Loggen Sie sich einfach über MyAccount ein und schon können Sie auf den Artikel HAFNIUM Malware BlackBerry Optics Rules (000075912)[6] in der Knowledge Base zugreifen.

---

[1] HAFNIUM targeting Exchange Servers with 0-day exploits

[2] New nation-state cyberattacks

[3] On-Premises Exchange Server Vulnerabilities Resource Center

[4] Government briefed on breach of at least 30,000 Microsoft Exchange Servers

[5] BlackBerry Offers Advanced AI Protection Against HAFNIUM Attacks

[6] HAFNIUM Malware Optics Rules Knowledge Base (KB) article (000075912)

- **BlackBerry® Guard** ist eine zuverlässige MDR-Lösung mit 24h-Support, die von BlackBerry Incident Response (IR)- und Präventionsexperten betreut wird. BlackBerry Guard schützt Sie vor HAFNIUM durch:
  - Überwachung und Auswertung von Warnmeldungen in Echtzeit
  - Einsatz korrigierender Richtlinien bei der Entdeckung von Lücken in der Richtlinienimplementierung
  - Bedrohungssuche nach Risikopriorisierung
  - Bereitstellung neuester Bedrohungsdaten und dazugehöriger Handlungsempfehlungen

Falls Sie befürchten, Opfer eines HAFNIUM-Angriffs geworden zu sein, lesen Sie das Microsoft-Dokument *HAFNIUM targeting Exchange Servers with 0-day exploits*[7] und insbesondere den Abschnitt „Indicators of Compromise".

Das BlackBerry IR-Team steht Ihnen bei der Bewertung und Verbesserung Ihres Endpoint-Schutzes zuverlässig zur Seite. Auch bei der Sicherheit, Integrität und Resilienz Ihrer Infrastruktur unterstützen wir Sie gern. Und zwar unabhängig von der Unternehmensgröße und Branche.

[7] HAFNIUM targeting Exchange Servers with 0-day exploits

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.

BlackBerry. Intelligent Security. Everywhere.

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

BlackBerry
Intelligent Security. Everywhere.