Whitepaper

Bitdefender®

JETZT NOCH MEHR SICHERHEIT DANK ENDPUNKT-RISIKOANALYSEN

Contents

Compliance heißt nicht automatisch, dass Sie auch abgesichert sind

Dieser Tage finden sich immer mehr Medienberichte über Cyberangriffe und große Mengen an gestohlenen Daten. Branchenstatistiken belegen, dass sich die Anzahl der durch derartige Sicherheitsverstöße exponierten Datensätze 2018 gegenüber 2017 mehr als verdoppelt hat. Ein genauerer Blick auf die medienwirksamsten Angriffe der letzten Zeit zeigt, dass viele der nennenswerteren Angriffe Unternehmen mit umfassenden Compliance-Anforderungen wie Target und Equifax betrafen. Darin wird deutlich, dass allein die Erfüllung von gesetzlichen Anforderungen keine Garant dafür ist, dass Cyberangriffe verhindert werden können. Denn Compliance heißt nicht, dass Sie sicher sind. Cyberkriminelle interessieren sich nicht für die Cybersicherheitsanforderungen und -standards Ihres Unternehmens. Cyberkriminellen geht es nur darum, Schwachstellen oder gefährdete Endpunkte in Ihrer Umgebung zu finden und für ihre Zwecke auszunutzen. Expertenanalysen deuten darauf hin, dass viele dieser Verstöße einen gemeinsamen Nenner hatten: Sie nutzten einen "gefährdeten Endpunkt", um sich Zugang zur Unternehmensumgebung zu verschaffen.

In einer typischen Unternehmensumgebung finden sich eine große Vielfalt an unterschiedlichen Assets. Ist ein solches Asset über das Internet erreichbar, gehen die möglichen Angriffsvarianten in die Hunderte. Schwache Passwörter, Sicherheitslücken in Software, Fehlkonfigurationen und zahlreiche andere Vektoren können genutzt werden, um sich einen ersten Zugang zum Netzwerk zu verschaffen. Ist dies erst einmal geschafft, kann sich der Angreifer schnell weiterbewegen. Findet er ein höherwertiges Asset und kompromittiert es, kommt es zu einer wirklich schwerwiegenden Sicherheitsverletzung. Die Zahl der möglichen Permutationen und Kombinationen verschiedener Angriffsverfahren, aus denen sich Angreifer für Kompromittierungen Ihrer Umgebung bedienen kann, geht in die Millionen.

Die meisten Datenschutzverletzungen sind eine direkte Folge des mangelnden Verständnisses für Angriffsflächen und gefährdete Endpunkte, das in vielen Unternehmen vorherrscht. Es ist sehr schwierig, festzustellen, welchen Sicherheitsrisiken ein Unternehmen konkret ausgesetzt ist, oftmals tappen die Verantwortlichen im Dunkeln.

Allgegenwärtige Herausforderungen

Unternehmen aller Größenordnungen treiben die digitale Transformation und den Umstieg auf Cloud- und mobile Lösungen immer weiter voran, wodurch ihre IT-Infrastrukturen immer größer und immer komplexer werden. Das belegt auch eine ESG-Umfrage: 68 % der Befragten gaben an, dass ihre IT-Umgebung in den letzten zwei Jahren an Komplexität zugenommen hat.

Abbildung 1.

Die Angriffsfläche wird immer größer

Die Zeiten, in denen Cybersicherheit lediglich den Schutz Ihrer Endpunkte und die Überwachung interner Netzwerke hinter der Firewall beinhalte, sind längst vorbei. Mit dem Wachstum von Unternehmen im Internet und in der Cloud ist auch ihre Angriffsfläche förmlich explodiert. Für erfinderische Hacker eröffnen sich durch diese enormen Angriffsflächen und die steigende Komplexität ganz neue Möglichkeiten.

Die digitalen Umgebungen moderner Unternehmen müssen auch mit externen Diensten verbunden sein. Dies geschieht meist in Form von selbst entwickelten und in der Cloud gehosteten Anwendungen oder durch die Verbindung mit Verbundanwendungen von Drittanbietern. Ein der wichtigsten Herausforderungen für IT- und Sicherheitsadministratoren besteht darin, einen eindeutigen und genauen Überblick über die Angriffsfläche des Unternehmens zu erhalten, risikobehaftete Endpunkte in der Umgebung zu identifizieren und falsch konfigurierten Endpunkten auf die Spur zu kommen.

Um sich vor Angriffen zu schützen, muss die Unternehmenssicherheit mehr als nur den Schutz von Endpunkten weiterentwickeln. Es bedarf einer vollkommen neuen Perspektive, die versteht, dass der Endpunktumgebung und den installierten Anwendungen ein weitaus größere Rolle zukommt, als den meisten bewusst ist. Das Denken in Bezug auf den reinen Endpunktschutz funktioniert nicht mehr. Um das Risiko für das Unternehmen wirklich zu verstehen und die Kontrolle über die Angriffsfläche zu behalten, benötigen Sie genaue Einblicke die Assets des Unternehmens und ihre Konfiguration ebenso wie in in die eingesetzten Anwendungen, Sicherheitsmaßnahmen, das Benutzerverhalten und vieles mehr.

Sicherheitsexperten sind schwer zu finden

In einer aktuellen Umfrage der ESG zu den drängendsten Herausforderungen von IT-Organisationen sollten die Teilnehmer die Bereiche ihre Unternehmens benennen, die von einem problematischen Fachkräftemängel betroffen sind. Bei 53 % der Befragten führte in den Jahren 2018-2019 der Bereich Cybersicherheit die Liste an. Mit 38 % belegen Fachkräfte für IT-Architektur und -Planung den zweiten Platz. Besonders besorgniserregend ist dabei die Tatsache, dass der Fachkräftemangel im Bereich Cybersicherheit in der von ESG jährlich durchgeführten Umfrage durchgehend den ersten Platz belegt. Schlimmer noch, der Anteil der Unternehmen, die einen problematischen Mangel an Cybersicherheitsexpertise angeben, nimmt immer weiter zu.

Dieser akute weltweite Fachkräftemangel birgt für Unternehmen ein erhöhtes Risiko für Cyberangriffe. Berichten zufolge werden die weltweiten jährlichen Kosten durch Cyberkriminalität bis 2020 voraussichtlich $2 Billionen US-Dollar übersteigen. Diese steigenden Qualifikationsdefizite führen dazu, dass das Risiko durch Cyberkriminalität steigt und Unternehmen einem erhöhtem Risiko für ihre Infrastruktur und Kunden ausgesetzt sind. Unternehmen, die Stellen neu besetzen wollen, benötigen oft sechs bis neun Monate, um qualifizierte Kandidaten zu finden. Dies hat schwerwiegende Auswirkungen und zwingt Unternehmen, in einem gefährlich unterbesetzten Umfeld zu agieren. Immer mehr IT-Sicherheitsteams müssen in der Folge ohne die notwendige Expertise in den Bereichen Analytics, forensische Untersuchungen und Cloud Computing auskommen. Darüber hinaus wird angesichts des Drucks auf die vorhandenen Ressourcen wenig Zeit in die kontinuierliche Schulung der Cybersicherheit investiert, und die Arbeitszufriedenheit der bestehenden Cybersicherheitsmitarbeiter kann leiden.

Zu viele Tools

Das "Shiny Object Syndrome", also der Hang, in alle möglichen neuen Tools und Technologien zu investieren, macht auch vor der Cybersicherheit nicht halt. Der Markt ist voll von Versprechungen zur Lösung der vielen Probleme der Informationssicherheit und findet auch immer wieder Abnehmer. Ist auch Ihr Sicherheitsteam von der schieren Anzahl der Sicherheitstools überwältigt? Verliert es den Überblick über die vielen nicht verwalteten Tools? Ist es nicht mehr ausreichend in der Lage, mit den vielen Informationen, Verfahren und Updates Schritt zu halten?

Die jüngste ESG-Umfrage kommt zu dem Ergebnis, dass 40 % der IT-Sicherheitsteams zwischen 10 und 25 Sicherheitstools verwenden, weitere 30 % verwenden ganze 26 bis 50 Werkzeuge. Diese Zahlen fallen im Finanzwesen sogar noch höher aus: Hier setzen 73 % der Unternehmen auf 35 oder mehr Tools. Dabei ist die hohe Anzahl der Tools allein kein Problem; das Problem liegt viel mehr in der mangelnden Integration dieser Tools und in ihren voneinander getrennten Funktionalitäten (https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf).

Wie funktionieren Cyberangriffe heute?

Der Ransomware-Angriff durch WannaCrypt (WannaCry) verursachte im Jahr 2017 weltweit verheerende Schäden. WannaCry ist ein Ransomware-Wurm, der sich schnell über Computernetzwerke hinweg verbreitet. Hat er einen Windows-Computers infiziert, verschlüsselt er im Anschluss Dateien auf der Festplatte und macht sie für Benutzer unzugänglich. Die Angreifer fordern dann ein Bitcoin-Lösegeld zur Entschlüsselung der Dateien.

Die WannaCry-Ransomware besteht aus mehreren Komponenten. Sie erreicht den infizierten Computer in Form eines Droppers, einer Ransomware-Komponente, die die Dateien auf dem Endpunkt verschlüsselt, sowie einer Wurmkomponente, die weitere verbundene Systeme infiziert, indem sie eine nicht gepatchte SMB-Schwachstelle in MS Windows-Systemen ausnutzt.

Sobald ein Endpunkt infiziert ist, versucht WannaCry, eine hartcodierte URL (Kill-Switch) aufzurufen. Falls diese URL nicht erreichbar ist, sucht und verschlüsselt die Ransomware-Komponente Dateien in verschiedenen gängigen Formaten, so zum Beispiel Microsoft Office-Dateien, JPEGs, MP3s und MKVs, so dass sie für den Benutzer nicht mehr zugänglich sind. Im Anschluss wird eine Geldforderung angezeigt: Der Nutzer wird aufgefordert Bitcoin im Gegenwert von 300 US-Dollar zu zahlen, damit die Dateien entschlüsselt und wiederhergestellt werden.

Die Ausbreitung von WannaCry hätte sich verhindern lassen

Die Wurmkomponente, die für die Weiterverbreitung verantwortlich ist, basiert auf dem Exploit einer SMB-Schwachstelle, der unter dem Namen EternalBlue bekannt wurde. Es wird angenommen, dass er ursprünglich von der U.S. National Security Agency entwickelt wurde. Dieser Exploit wurde von einer Hackergruppe namens Shadow Brokers gestohlen und im Darknet veröffentlicht. Wurde er in ein Windows-Netzwerk eingeschleust, gelang es WannaCry, sich selbst zu verbreiten und andere nicht gepatchte Computer ohne menschliches Eingreifen zu infizieren. Diese Fähigkeit zur Selbstausbreitung trug zu seinem raschen Erfolg bei.

Ironischerweise entdeckte Microsoft diese Schwachstelle selbst und veröffentlichte umgehend einen Patch, der in der Lage ist, WannaCry schon vor Beginn des Angriffs zu verhindern. Das am 14. März 2017 veröffentlichte Microsoft Security Bulletin MS17-010 sollte mit dem Update der Windows-Version des SMB-Protokolls eine Infektion über EternalBlue ausschließen. Obwohl Microsoft den Patch als kritisch eingestuft hatte, waren viele Systeme noch nicht gepatcht, als im Mai 2017 die schnelle Ausbreitung von WannaCry begann. Für nicht gepatchte Systeme, die infiziert werden, gibt es wenig Abhilfe, außer der Wiederherstellung von Dateien aus einem sicheren Backup - und der Erkenntnis, nie wieder ein Sicherheitspatch auszulassen.

Trotz aller öffentlichen Aufmerksamkeit - ganz zu schweigen von den vorbeugenden Patches und Best Practices - infiziert WannaCry auch heute noch Systeme. Nicht, weil es kein Gegenmittel gibt, sondern weil diese Patches viel zu oft nicht eingespielt werden, kann Malware wie WannaCry auch noch lange nach Veröffentlichung einer Problemlösung weiterhin Schäden verursachen. Die macht deutlich, wie wichtig es ist, die Risiken, die von den Endpunkten in Ihrer Umgebung ausgehen, zu kennen und sie rechtzeitig anzugehen.

Die weitaus größere Gefahr geht heute von WannaCry-Varianten, oder genauer gesagt, von neuer Malware aus, die auf dem gleichen EternalBlue-Wurmcode wie WannaCry basiert. Alle auf EternalBlue basierten Malware-Programme nutzen die gleiche Windows-Schwachstelle aus. Die Tatsache, dass diese Angriffe weiterhin zunehmen, deutet also darauf hin, dass es immer noch viele nicht gepatchte Windows-Systeme gibt. Es ist nur eine Frage der Zeit, dass ein Angreifer sie findet.

Die wichtigsten Anforderungen an die Endpunktsicherheit

Endpunkt-Risikoanalysen und -Hardening

Für einen umfassender Ansatz zur Absicherung ihrer Umgebungen müssen Unternehmen zunächst verstehen, wo die Angriffsflächen liegen, um dann gefährdete Endpunkte zu identifizieren und zu härten und so ihre Anfälligkeit für Cyberangriffe zu minimieren. Bei Bitdefender betrachten wir dies als den ersten Schritt auf dem Weg zu umfassender Sicherheit.

Die Hardening von Endpoints ist ein Verfahren zur Reduzierung ihrer Angriffsfläche durch:

Operating System Hardening – Das Betriebssystem mit den neuesten Funktionalitäten auf dem aktuellsten Stand halten, unnötige Programme, Sicherheitsfunktionen, Konfigurationen usw. entfernen.

Services Hardening – Deaktivieren unnötiger und unerwünschter Dienste, Prozesse, Funktionen und Funktionalitäten.

Analyse von Endpunktfehlkonfigurationen - Durchgehende Überwachung der Endpunkte auf Fehlkonfigurationen, gefolgt von Berichterstattung und Behebung.

Application Hardening - Anwendungen mit den neuesten Patches und Bugfixes auf den aktuellsten Stand halten.

Viele Unternehmen verwenden in das Betriebssystem integrierte Tools bzw. von Betriebssystemherstellern angebotene Tools wie Microsoft SCCM, um das Betriebssystem auf dem neuesten Stand zu halten. Andere wiederum setzen auf Patch-Management-Lösungen von Drittanbietern, die darauf ausgelegt sind, das Betriebssystem und die gängigsten Anwendungen zu patchen. Es gibt jedoch nur wenige Tools, mit denen Fehlkonfigurationen von Endpunkten ermittelt und behoben werden können. Ein solches Tool ist das erst kürzlich angekündigte Microsoft Defender ATP Threat & Vulnerability Management, das den Endpunkt auf Fehlkonfigurationen von Betriebssystem und Anwendungen sowie fehlende Updates/Patches überprüft und aus diesen Informationen einen Schwachstellenindex erstellt.

Die wenigen Tools, die einige oder alle dieser Hardening Aktivitäten umfassen, sind voneinander isoliert, mit jeweils eigenen Managementkonsolen ausgestattet und werden in der Regel von verschiedenen Teams verwaltet. Dies führt zu Unübersichtlichkeit und Verzögerungen und hinterlässt Lücken im Schutz. Abhilfe kann hier nur eine integrierte Lösung für lückenlose Sicherheit schaffen.

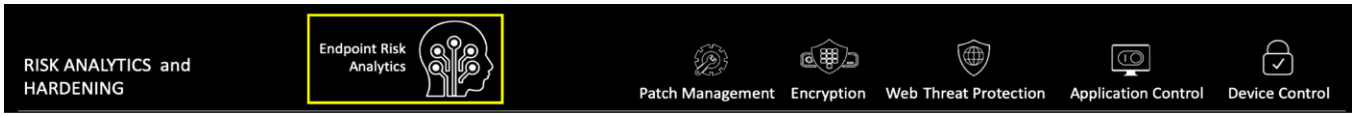
Integrierte risikogesteuerte Prävention

Die Sicherheitsanforderungen eines Unternehmens werden durch eine Vielzahl von Faktoren bestimmt. So gibt es Unternehmen, wie beispielsweise im Finanz- und Gesundheitssektor, deren Cybersicherheitsanforderungen auf die Einhaltung gesetzlicher Vorschriften ausgelegt sind. Andere Unternehmen wiederum richten ihre Anforderungen an bereits erlebten Sicherheitsverletzungen aus oder versuchen, diese proaktiv zu vermeiden.

Und obwohl diese Ansätze durchaus hilfreich sind, reichen sie nicht aus, um umfassende Sicherheit zu garantieren, da sie viel zu eng gefasst sind. Ein zielführender Weg zur Gewährleistung umfassender Sicherheit liegt in einem ganzheitlichem Ansatz, der neben der Identifizierung gefährdeter Assets in Unternehmensumgebungen auch eine kontinuierliche Bewertung aller Endpunkte auf Schwachstellen und Sicherheitseinstellungen umfasst und entweder automatisierte oder unterstützte Abhilfemaßnahmen sowie optimale Prävention und Transparenz bietet.

GravityZone gibt IT-Team Tools an die Hand, mit denen sie ihre Sicherheitsprozesse auf ein neues Niveau heben können. Endpunkt-Risikoanalysen gehören zu den neuesten Technologien, die wir in den Hardening Prozess unserer Sicherheitslösung aufgenommen haben, neben anderen bewährten Funktionen wie Full Disk Encryption, Internet-Bedrohungsschutz, Gerätesteuerung, Anwendungssteuerung und Patch Management.

Abbildung 2.



So funktionieren die Bitdefender-Risikoanalysen

Die GravityZone-Risikoanalysen überprüfen alle geschützten Endpunkte kontinuierlich auf über 200 Risikoindikatoren und errechnet daraus aggregierte Risikobewertungen sowie endpunktspezifische Bewertungen. Diese Werte werden dann im Risiko-Dashboard zusammen mit der Schwere des Risikos angezeigt. Aktuell basieren die in der Risikoanalyse verwendeten Kriterien hauptsächlich auf der Identifizierung von Fehlkonfigurationen auf den Endpunkten, da diese der häufigste Grund für Sicherheitsverletzungen sind.

Endpoint Fehlkonfigurationen

Die Fehlkonfiguration von Systemen ist ein zentraler Grund dafür, dass es auf Endpunkten zu Sicherheitsverletzungen kommt - mehr als 90 % vergangener Cybersicherheitsangriffe waren überhaupt erst möglich, weil ein Endpunkt in der Umgebung falsch konfiguriert war oder eine Einstellung übersehen wurde und sich ein Angreifer auf diesem Wege Zugriff verschaffen konnte.

Hier einige Beispiele für Systemfehlkonfigurationen, die von Angreifern ausgenutzt werden können:

- **Die Deaktivierung des erweiterten Schutzes**
- **Aktivierung des Windows Telnet Service** für unverschlüsselte eingehende Verbindungen anstelle von SSH-Servern, was den unbefugten Zugriff Dritter auf den Computer ermöglicht.
- **Die Aktivierung der automatischen Anmeldung?ACE 3?> reduziert den Kontoschutz und macht es für jeden zugänglich.**
- **Die unzureichende Absicherung oder Deaktivierung der Benutzerkontensteuerung (UAC)**, so dass der Benutzer nicht über Dritte informiert wird, die versuchen, neue Software zu installieren oder Computereinstellungen zu ändern.
- **Die Aktivierung des LM-Hashes**, obwohl er standardmäßig deaktiviert sein sollte, um die Passwortverschlüsselung und Authentifizierung nicht zu beeinträchtigen.
- **Deaktivierung der zufälligen Anordnung des Layouts des Adressraums (Address Space Layout Randomization, ASLR)** beeinträchtigt die Systemsicherheit und sollte immer aktiviert sein.
- **Die Deaktivierung des Sitzungs-Manager-Schutzmodus**
- **Die Aktivierung der unsicheren Gastanmeldung** schwächt die Sicherheit von Windows-Clients. Die unsichere Gastanmeldung sollte niemals aktiviert werden, da Gastkonten anfälliger für Man-in-the-Middle-Angriffe sind.
- **Keine Deaktivierung der Autorun-Funktion** – diese Funktion sollte deaktiviert werden, da sie ansonsten die Ausführung von Code durch Angreifer ohne Eingreifen oder Wissen des Benutzers ermöglicht.

Wenn eine dieser Bedingungen oder der anderen 206 vordefinierten Bedingungen auf dem Endpunkt vorliegt, erhöht sich der Risikowert des Endpunkts um einen festgelegten Wert, der sich aus dem Schweregrad der jeweiligen Bedingung ergibt.

Dank Endpunkt-Risikonanalysen können IT-Administratoren ab sofort die allgemeine Sicherheitslage ihres Unternehmens einschätzen. Der im zentralen Dashboard angezeigte Gesamtrisikowert ergibt sich aus den Risikowerten der einzelnen Endpunkte. Über die Benutzeroberfläche der Endpunkt-Risikoanalyse können Administratoren per Drilldown vom Gesamtrisikowert zu den Risikowerten der einzelnen Endpunkte gelangen.

Das Risiko-Dashboard von GravityZone gibt IT-Administratoren wie in der folgenden Abbildung dargestellt (Abbildung 3) detaillierte Einblicke in das Risikoprofil aller durch GravityZone geschützten Endpunkte. Das zentrale Risiko-Dashboard liefert ein allgemeines Risikoprofil. Die oberste Zeile zeigt die Gesamtzahl der geschützten Geräte, den Status und die Entwicklung der Risikobewertung, Geräte nach Betriebssystem und den Gerätetyp (Endpunkt oder Server) sowie weitere Informationen an.

Abbildung 3.

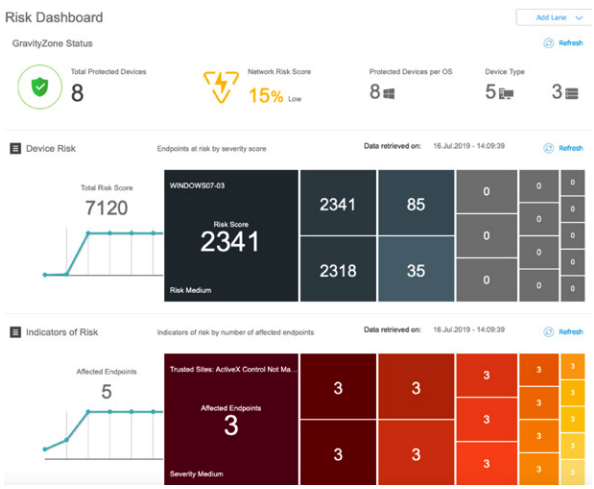


Abbildung 4.

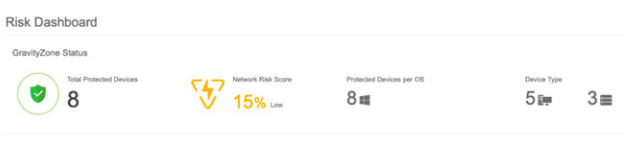
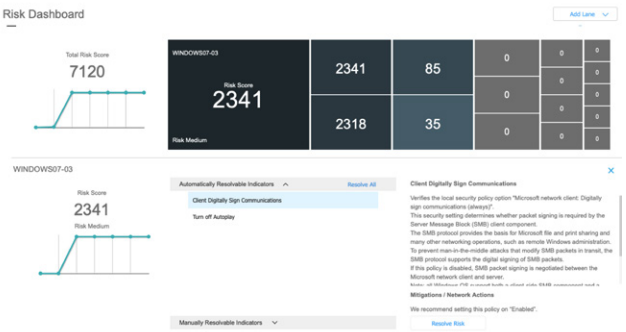


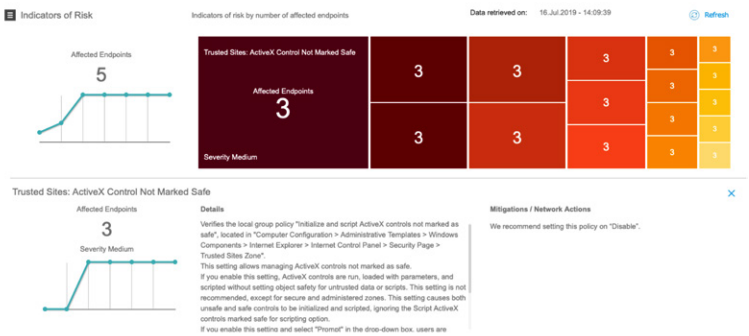
Abbildung 5.



Die zweite Zeile (Abbildung 5) zeigt die Gesamtrisikobewertung an. Auf den Kacheln finden sich die Risikobewertungen der einzelnen Endpunkte, absteigend von links nach rechts sortiert. Bewegt man die Maus über diese Kacheln, werden zusätzliche Details wie Name des Endpunkts, Art und Kategorie des Risikos usw. angezeigt. Mit einem Klick auf die Schaltfläche "Details" auf der Kachel wird eine detaillierte Beschreibung der Risiken zusammen mit optionalen Maßnahmen zur Behebung des Risikos (falls möglich) bzw. eine Schritt-für-Schritt-Anleitung zur Problembehebung angezeigt. Dadurch erhalten IT-Administratoren ein tieferes Verständnis für das Ausmaß der Risiken, denen ihre Endpunkte ausgesetzt sind, mit Informationen zur Behebung von sowie in einigen Fällen der Möglichkeit zur automatischen Behebung.

In der dritten Zeile des Risiko-Dashboards (Abbildung 6) werden die Risikoindikatoren angezeigt, die Aufschluss über die Arten von Risiken in der Unternehmensumgebung geben. Die Farbe der Kachel kennzeichnet den Schweregrad des Risikos und die Ziffern in der Mitte zeigen die Anzahl der betroffenen Endpunkte an. Mit einem Klick auf die Schaltfläche "Details" werden in einem neuen Fenster eine detaillierte Beschreibung dieser Risiken und gegebenenfalls geeignete Abhilfemaßnahmen angezeigt.

Abbildung 6.



Zusammenfassung

Wirksame Cybersicherheit lässt sich nicht allein durch den Einsatz von EPP- und EDR-Lösungen erreichen. Um auch neuen Bedrohungen immer einen Schritt voraus zu sein, sind Endpunkt-Risikoanalysen unerlässlich. Möglich wird dies, indem Endpunkte durchgehend auf verschiedene Risikokriterien überwacht werden, so zum Beispiel durch die Analyse von Endpunkt-Fehlkonfigurationenauf Grundlage der Security Baseline-Sicherheitsempfehlungen von Microsoft und anderen proprietären Kriterien zur Schwachstellenbewertung. Durch umfassende Risikoanalysen erhalten Administratoren Einblick in die allgemeine und spezifische Sicherheitslage der Endpunkte im Unternehmen. Die Endpunkt-Risikoanalyse ermöglicht eine automatische Behebung mit nur einem Klick für eine Vielzahlvon Risiken und schlägt Abhilfemaßnahmen für andere, komplexere Risiken vor (unterstützte Behebung). Durch die Identifizierung gefährdeter Endpunkte in Ihrer Unternehmensumgebung und die schnellstmögliche Behebung von Sicherheitslücken verringern Sie die Wahrscheinlichkeit von schwerwiegenden Sicherheitsverletzungen erheblich. Administratoren, die in der Lage sind, digitale Risiken im Unternehmen zu verwalten, können heute schon die Cyberangriffe von morgen verhindern.

Weitere Informationen finden Sie unter https://www.bitdefender.de/business/

Diese Seite ist absichtlich leer

Diese Seite ist absichtlich leer

Bitdefender ist ein international aufgestellter Anbieter von Sicherheitstechnologien, dessen Lösungen über ein umfangreiches Netzwerk aus Partnern, Händlern und Wiederverkäufern in über 100 Ländern verfügbar sind. Seit 2001 konnte Bitdefender immer wieder mit preisgekrönter Sicherheitstechnologie für Unternehmen und Privatanwender überzeugen und ist einer der führenden Anbieter von Sicherheitslösungen für Virtualisierungs- und Cloud-Technologien. Bitdefender-Technologie landet regelmäßig an der Spitze einschlägiger Tests und setzt den Maßstab in Sicherheitsstandards, die durch intensive Forschung und Entwicklung, Kooperationen und Partnerschaften selbst den höchsten Ansprüchen gerecht werden. Das gleiche gilt für die strategischen Partnerschaften mit den weltweit führenden Virtualisierungs- und Technologieanbietern. Weitere Informationen sind unter www.bitdefender.de verfügbar.

Bitdefender-WhitePaper-WOPERA-CREAT3370-de_DE