DELL Technologies

Sichern von Endpunkten angesichts neuer Bedrohungen

Wenn Unternehmen Mitarbeitern die Flexibilität geben, auch im Homeoffice vollständig produktiv zu arbeiten, müssen sie unbedingt sicherstellen, dass Endpoint-Security-Maßnahmen vorhanden sind, um der wachsenden Bedrohungslandschaft zu begegnen. Sie müssen Bedrohungen erkennen und darauf reagieren können, während sie gleichzeitig Flexibilität für das Arbeiten im Homeoffice bieten.

Während IT-Führungskräfte den Horizont auf das Ende der COVID-19-Pandemie absuchen, planen viele die neue Normalität mit einer weitaus höheren Anzahl von Homeoffice-Mitarbeitern als je zuvor. Während viele Unternehmen und ihre Mitarbeiter zwar von mehr Produktivität und einen flexibleren Arbeitsstil profitieren, muss ein Preis in puncto Schutz gezahlt werden. Die rasante Zunahme von Homeoffice-Arbeitsplätzen aufgrund von COVID-19 hat den Schutz von Endpunkten erschwert. 84 % der IT-Führungskräfte sagen, dass der Schutz von Homeoffice-Mitarbeitern schwieriger sei.[1] Eine mögliche Erklärung ist die Zunahme von Ransomwareangriffen auf weltweite Unternehmen bei Ausbruch der Pandemie um 148 %.[2] Diese Statistik ist besonders ernüchternd angesichts der Tatsache, dass Homeoffice-Mitarbeiter auf E-Mail als primäres Mittel für die geschäftliche Kommunikation vertrauen, was zu einer Zunahme von Phishingangriffen um 350 % geführt hat.[3]

Fortlaufende Trends bei der Cybersicherheit

Die plötzliche Umstellung auf das Arbeiten im Homeoffice findet vor dem Hintergrund vieler beunruhigender Cybersicherheitsbedenken statt, die das Fachwissen von Cybersicherheitsexperten strapazieren. Dazu zählen:

1. Angriffe auf BIOS-Level – ausgenutzte Sicherheitslücken in der Hardware oder auf dem Chip. Wenn das BIOS infiziert ist, bleibt der Angreifer oft verborgen, während der Gerät Zugriff über Zugangsdaten auf das Netzwerk und die Daten hat. 63 % der Unternehmen haben eine Datenschutzgefährdung oder -verletzung durch solche Angriffe erlebt.[4]
2. Advanced Persistent Threats (APTs) – ausgeklügelte Bedrohungen, die häufig im Hintergrund lauern, während sie verhaltensbezogene Informationen als Vorspiel für die Abschöpfung wertvoller Daten sammeln. Die Opfer erkennen möglicherweise lange Zeit – durchschnittlich 108 Tage[5] – nicht, dass ein verborgener Angriff stattgefunden hat.
3. Dateibasierte und dateilose Malware
   - Dateibasierte Malware – in der Regel Dateitypen mit vertrauten Erweiterungen wie DOCX und PDF – die Art von Dokumenten, mit denen Mitarbeiter ihre Arbeit erledigen. Wenn ein Nutzer die Datei öffnet, wird ein eingebetteter bösartiger Code ausgeführt.
   - Dateilose Malware – in der Regel ein legitimes Programm, mit dem ein Computer infiziert wird. Wenn der Nutzer ein solches Programm über eine E-Mail startet, infiziert die dateilose Malware den Computer und potenziell auch das Netzwerk, sodass viele Sicherheitstechnologien erfolgreich umgangen werden.
4. Von Nationalstaaten ausgehende Angriffe – typischerweise aus China, Nordkorea, Russland und dem Iran. Durch das technologische Fachwissen und die finanzielle Unterstützung dieser Nationalstaaten sind Angriffe oft raffiniert und sehr schädlich. Viele dieser Angriffe nutzen jedoch Systeme aus, bei denen die neuesten Updates und Patches fehlen. Die CISA-Einheit des FBI versendet regelmäßig Sicherheitsratgeber.

Die plötzliche Umstellung auf das Arbeiten im Homeoffice findet vor dem Hintergrund vieler beunruhigender Cybersicherheitsbedenken statt, die das Fachwissen von Cybersicherheitsexperten strapazieren.

1. „The State of DLP 2020“, Tessian.
2. VMware Carbon Black-Blog, Patrick Upatham und Jim Treinen, 15. April 2020.
3. Google-Bericht, zitiert in PCMAG.com, 30. März 2020.
4. „Match Present-Day Security Threats with BIOS-Level Control“, ein Thought Leadership-Whitepaper von Forrester Consulting im Auftrag von Dell, Juni 2019.
5. The 2018 U.S. State of Cybercrime Survey.

5. Cloud-basierte Angriffe – auf dem Vormarsch, da Desktopanwendungen immer mehr durch Cloud-basierte Anwendungen für die Zusammenarbeit und Produktivität ersetzt werden. Bei einer Nutzung von mehr als 2.400 Cloud-Services im durchschnittlichen Unternehmen bestehen in 93 % der Unternehmen moderate oder extreme Bedenken bezüglich der Cloud-Sicherheit.[6] Schutzmaßnahmen müssen DLP-Funktionen (Data Loss Prevention) und Bedrohungsschutz in der Cloud umfassen. Darüber hinaus muss die Nutzerauthentifizierung vor Spoofing geschützt werden und Daten müssen auf ihrem Weg in die und aus der Cloud verschlüsselt werden.

6. Compliancebestimmungen – für den Schutz personenbezogener Daten. Um zu verhindern, dass personenbezogene Daten in die falschen Hände geraten und letztendlich für Identitätsdiebstahl verwendet werden, haben einige Branchen strenge Bestimmungen eingeführt, die harte Strafen enthalten. Dazu gehören HIPAA im Gesundheitswesen, PCI-DSS bei Finanzdienstleistungen und im Einzelhandel sowie die DSGVO für Unternehmen, die Geschäfte mit europäischen Bürgern abwickeln.

7. Lähmende Risiken – resultierend aus prognostizierten Verlusten durch Cyberkriminalität in Höhe von 6 Billionen US-Dollar im Jahr 2021, eine Steigerung gegenüber 3 Billionen US-Dollar im Jahr 2015. Laut Cybersecurity Ventures sind die Verluste auf Schäden und Vernichtung von Daten, gestohlene Gelder, Produktivitätseinbußen, Diebstahl von geistigem Eigentum, Diebstahl von persönlichen und finanziellen Daten, Unterbrechungen nach Angriffen, Rufschädigungen und mehr zurückzuführen.[7]

Überdenken der Endpoint Security

Endpoint Security: Teil der Unternehmenssicherheit
Angesichts einer größeren Anzahl von Homeoffice-Mitarbeitern als je zuvor, von denen viele mit sensiblen Daten arbeiten müssen, um ihre Aufgaben erledigen zu können, sollten IT-Führungskräfte den aktuellen Status der Endpoint Security in ihren Unternehmen bewerten.
Statt sich aber die Endpoint Security an sich anzusehen, sollten sie diese als wesentlichen Bestandteil der Unternehmenssicherheit betrachten, um einen weitreichenden Schutz zu implementieren. Sie sollten außerdem über die Endpunkte hinausgehen und Storage, Netzwerke sowie Cloud-basierte Services einbeziehen. Ein ganzheitlicher Ansatz für „vertrauenswürdige Geräte“ innerhalb des Unternehmens muss die folgenden Faktoren berücksichtigen:

Integrierte Sicherheit
Statt ausschließlich auf Software für den Schutz von Endpunkten zu vertrauen, erfordert ein umfassender Ansatz die Nutzung von vertrauenswürdigen Geräten – also von Endnutzer-Computing-Geräten, bei denen Sicherheit in die Geräte an sich implementiert ist. Solche Geräte schützen personenbezogene Daten und spielen eine wichtige Rolle im Hinblick auf die Einhaltung der Compliance, wenn ein Gerät verloren geht oder gestohlen wird. Endnutzergeräte sollten außerdem Datenschutzfiltertechnologie umfassen, die dafür sorgt, dass Kollegen und Bürobesucher nur begrenzt vertrauliche Informationen auf einem Computerbildschirm sehen können.

IT-Führungskräfte sollten Endpoint Security als wesentlichen Teil der Unternehmenssicherheit betrachten.

6. Cybersecurity Insiders Cloud Security Reports, 2018, 2019.

7. Cybersecurity Ventures, 2020.

Schutz oberhalb und unterhalb des BS

Oberhalb des BS: Die IT benötigt Transparenz, Monitoring und Datensicherheit sowie die Möglichkeit, Bedrohungen zu verhindern, zu erkennen und zu beheben. Eine Verschlüsselung auf dem Gerät ist ebenfalls sehr wichtig, um Complianceanforderungen zu erfüllen, sollte aber nicht die Performance beeinträchtigen, damit die Nutzerproduktivität nicht verringert wird.

Unterhalb des BS: Die IT benötigt BIOS-Schutz und Chipauthentifizierung aufgrund der Häufigkeit von Angriffen auf Firmware und Hardware. Ein infiziertes BIOS verschafft Angreifern Zugriff auf alle Daten auf einem Endpunkt, einschließlich Zugangsdaten, sodass Angreifer sich innerhalb des Netzwerks eines Unternehmens bewegen und die breitere IT-Infrastruktur angreifen können.

KI und ML

Angesichts der zunehmend raffinierten Angriffe von heute ist die Nutzung von künstlicher Intelligenz und maschinellem Lernen bei der Erkennung und Korrektur unerlässlich für den Endpunktschutz. Durch Beobachtung von Verhaltensmustern können KI- und ML-Algorithmen ungewöhnliche Aktivitäten erkennen, die eine Sicherheitsverletzung aufzeigen und verhindern könnten.

Sichere Lieferkette

Im Fertigungsprozess können böswillige Akteure infizierte Komponenten einbringen, um einen Backdoor-Angriff zu ermöglichen. Nach der Einbettung in ein gefertigtes Produkt können diese Komponenten eine Sicherheitsverletzung ermöglichen, die extrem schädlich und schwer zu erkennen sein kann. Daher ist es sowohl für Lieferanten als auch Hersteller von entscheidender Bedeutung sein, strenge Sicherheitsmaßnahmen an kritischen Punkten in der Lieferkette zu implementieren.

Vertrauenswürdige Geräte schützen personenbezogene Daten und spielen eine wichtige Rolle im Hinblick auf die Compliance, falls ein Gerät verloren geht oder gestohlen wird.

Dell Trusted Devices

Dell integriert mit den folgenden Technologien Sicherheit in jeden PC:

SafeBIOS mit BIOS-Angriffsindikatoren (Indicators of Attack, IoA) bietet transparente Einblicke in BIOS-Änderungen, um Manipulationen zu verhindern. Dell verwaltet ein geschütztes Image unabhängig vom Host, um die Integrität des BIOS zu überprüfen SafeBIOS ist jetzt in VMware Carbon Black Audit and Remediation integriert, wodurch mehr transparente Einblicke in Angriffe durch automatisiertes Reporting ermöglicht werden. Zudem kann eine BIOS-Infizierung durch Remotezugriff behoben werden.

SafeID bietet eine chipbasierte Authentifizierung. Die Endnutzerzugangsdaten werden mithilfe eines speziellen Sicherheitschips überprüft, statt auf Software zu vertrauen, die weniger sicher ist.

SafeScreen schützt Bildschirme, auf denen vertrauliche Informationen für Kollegen im Büro, Besucher, Wartungsmitarbeiter oder andere nicht autorisierte Personen sichtbar sein könnten.

SafeGuard and Response: Das von VMware Carbon Black- und Secureworks-Technologien unterstützte Dell Portfolio umfasst Folgendes:

VMware Carbon Black ist eine Cloud-native Plattform für den Endpunktschutz, die ein intelligentes Härten des Systems und einen Verhaltensschutz umfasst, die erforderlich sind, um aufkommende Bedrohungen mithilfe eines einfachen Agent und einer benutzerfreundlichen Konsole in Schach zu halten.

Secureworks Managed Services erfassen Telemetriedaten aus der Cloud, aus dem Netzwerk und vom Endpunkt und fassen diese zusammen, um Bedrohungen für das gesamte Unternehmen zu identifizieren. Secureworks Managed Services bieten eine branchenführende Reaktion auf Incidents und sind in die VMware Carbon Black-Plattform und viele weitere Plattformen integriert.

SafeData: Zusammenarbeit, die seit jeher ein Kennzeichen erfolgreicher Unternehmen ist, gewinnt im Zeitalter des intensivierten Arbeitens im Homeoffice zusätzlich an Bedeutung. Die heutige Zusammenarbeit von Mitarbeitern erfordert eine Datensicherheit sowohl auf dem Gerät als auch in der Cloud, die den Endnutzer nicht beeinträchtigt. Dell arbeitet mit Netskope und Absolute zusammen, um eine ganzheitliche Endpoint Security bereitzustellen.

Netskope: Mit einem datenzentrierten Ansatz schützt die Netskope-Technologie Daten, die in der Cloud erstellt und zur Verfügung gestellt werden. Netskope stellt der IT transparente Einblicke in Echtzeit, Zugriff auf die Cloud, Monitoring und die Vermeidung von Datenverlusten bereit und definiert so die Cloud-, Netzwerk- und Datensicherheit neu. Teams werden mit der richtigen Balance zwischen Schutz und Geschwindigkeit unterstützt, sodass sie die digitale Transformation ihres Unternehmens sichern können.

Absolute: Dell integriert Absolute-Technologie in die Firmware jedes Geräts und stellt damit jedem Endpunkt eine Verknüpfung zur automatischen Fehlerkorrektur zum Cloud-basierten Absolute-Dashboard bereit. Damit können Manager Endpunkte und die darauf liegenden Daten nachverfolgen, managen und sichern, selbst wenn sie sich außerhalb des Netzwerks befinden. Technologie von Absolute bietet die folgenden Funktionen:

- Suche und Management von Geräten
- Bereitstellung von Persistenz für das VPN und Sicherheitssoftware
- Implementierung eine Air-Gap-Lösung zur Unterstützung der Recovery nach Angriffen
- Multi-Cloud-Data-Protection-Lösungen, die software- oder Appliance-basiert sein können

Fazit

Die rasante Zunahme von Homeoffice-Arbeitsplätzen aufgrund der COVID-19-Pandemie erhöht die Gefahren in einer bereits an Bedrohungen reichen Cybersicherheitslandschaft. Es ist ein neuer, ganzheitlicher Ansatz für den Endpunktschutz erforderlich. Das Überdenken des Endpunktschutzes beginnt mit vertrauenswürdigen Geräten, die sowohl oberhalb als auch unterhalb des Betriebssystems geschützt sind. Eine solche Strategie geht über die Endpunkte an sich hinaus, um unternehmensweite Einblicke in die Cybersicherheit bereitzustellen, die Server, Netzwerke, Cloud-basierte Services und Compliance umfasst. Das Portfolio an vertrauenswürdigen Dell Geräten stellt einen solch umfassenden Ansatz dar. Der Endpunktschutz von Dell umspannt das gesamte Unternehmen und umfasst Multi-Cloud-Data-Protection-Lösungen, die als software- und/oder Appliance-basierte Lösungen bereitgestellt werden können. Vor allem ermöglichen vertrauenswürdige Dell Geräte es Nutzern aber, hochgradig produktiv zu bleiben, indem sie die zunehmend raffinierten Angriffe im neuen Paradigma des Arbeitens im Homeoffice bezwingen.

Weitere Informationen finden Sie unter:
https://www.delltechnologies.com/de-de/endpoint-security/index.htm

Die heutige Zusammenarbeit von Mitarbeitern erfordert eine Datensicherheit sowohl auf dem Gerät als auch in der Cloud, die den Endnutzer nicht beeinträchtigt.