DELL Technologies

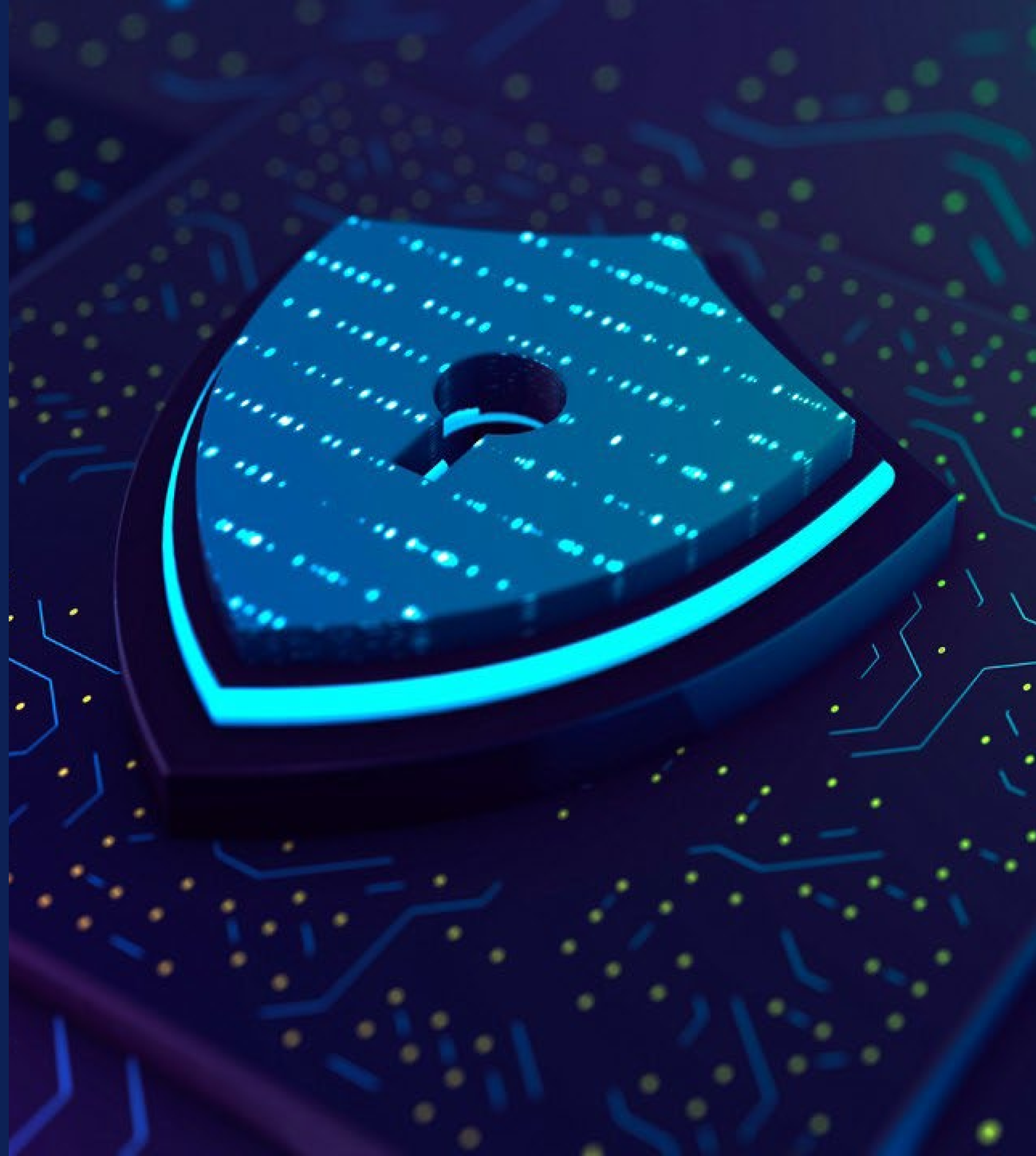
intel. Accelerate AI with Intel®

Windows 11

Die Gestaltung einer sicheren Arbeitsumgebung

Sorgen Sie mit Abwehrmaßnahmen auf mehreren Ebenen für mehr Sicherheit in Ihrer gesamten Flotte.

Inhalt



Zusammenfassung

Cyberangriffe sind unvermeidbar – und sie nehmen an Häufigkeit sowie Ausgereiftheit zu. Endgeräte, Netzwerke und Cloud-Umgebungen sind zu Hauptzielen geworden.

Dieses E-Book richtet sich an EntscheidungsträgerInnen in den Bereichen IT und Sicherheit. Es bietet eine Anleitung mit allen Elementen, die für den effektivsten Endpunktschutz in der sich stets weiterentwickelnden Bedrohungslandschaft erforderlich sind.

Inhaltsverzeichnis

Die Bedrohungslandschaft

Der Wechsel zum hybriden Arbeitsmodell hat zu mehr Komplexität und neuen Angriffsvektoren geführt – **Endpunkte, Netzwerke und Clouds bieten erweiterte Angriffsflächen**.

Zudem setzen AngreiferInnen nun ausgefeilte Techniken ein, die auf verschiedene Ebenen des Compute-Stacks abzielen und sich als valide Systemprozesse „tarnen“. Einige dieser Methoden ermöglichen den AngreiferInnen sogar privilegierten Zugriff, sodass sie den Softwareschutz *gänzlich unentdeckt* umgehen können.

Viele Unternehmen haben einen Zero-Trust-Weg eingeschlagen, um diese Bedrohungen zu bekämpfen. Allerdings ist es für die Umsetzung der Zero-Trust-Prinzipien erforderlich, das Gerätevertrauen zu wahren.

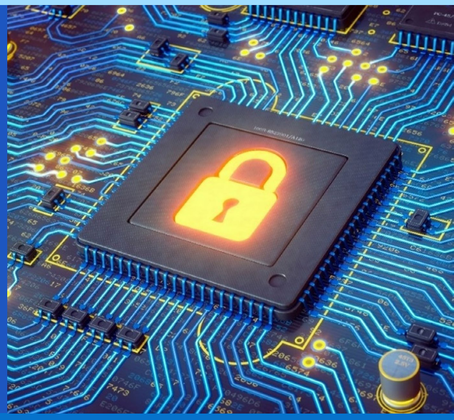
Aber wie wahren Sie das Gerätevertrauen, wenn Angriffe immer häufiger auftreten und moderne Technologie neue Angriffsvektoren erzeugt?

Dell und Intel wenden Zero-Trust-Prinzipien bei ihren PCs an, um Unternehmen und deren MitarbeiterInnen zu schützen.

Weitere Informationen

Schon gewusst?

71 % der Angriffe im Jahr 2022 basierten nicht auf Malware – eine Zunahme von 9 % ggü. dem Vorjahr.[1]



Nur 41 % der befragten Unternehmen können zweifelsfrei sagen, dass Sicherheit in ihre Technologie und Anwendungen integriert ist.[2]

Sie möchten mehr über Zero Trust erfahren, um die Ausgereiftheit Ihrer Cybersicherheit zu verbessern?

Lesen Sie unser E-Book:
Endpoint Security als wesentlicher Bestandteil von Zero Trust

1. CrowdStrike Global Threat Report, 2023.
2. Dell Innovation Index, 2023.

Herausforderungen

Für eine effektive Endpoint Security müssen Sie wissen, was AngreiferInnen motiviert und wie sie arbeiten.

Da eine Sicherheitsverletzung potenziell hohen Gewinn verspricht, **starten AngreiferInnen häufig mehrere Versuche beim selben Unternehmen. Dabei nutzen sie unterschiedliche Methoden und Einstiegspunkte, um ihre Erfolgschancen zu erhöhen.** Beispielsweise können die AngreiferInnen über den Lebenszyklus eines einzigen Geräts versuchen, die Sicherheitslücken über Dutzende Vektoren auszunutzen.

Legacy-Abwehrmaßnahmen reichen nicht mehr aus, um Endpunkte zu schützen. Wenn die Unternehmen die Abwehr einer Angriffsfläche verstärken, versuchen es die BedrohungsakteurInnen einfach bei leichteren Zielen. Mit dem Wechsel zur hybriden Arbeitswelt haben sie neue Angriffsvektoren für Endpunkte gefunden, die verheerende Ausfälle nach sich zogen.

Siehe Beispiele rechts

Angriff auf die Lieferkette: zielt auf Lieferanten ab, um Zugriff auf deren Systeme, Daten und/oder Netzwerk und, im Endeffekt, auf deren Kunden zu erhalten.

BEISPIEL: Angriff auf eine Hardwarelieferkette, ermöglicht durch die Manipulation einer Komponente:

Die AngreiferInnen fangen einen PC-Versand ab und tauschen die Festplatten.

Die IT stellt die kompromittierten Geräte im Unternehmen bereit.

Die AngreiferInnen installieren Malware, um die Zugangsdaten während des Anmeldevorgangs der NutzerInnen zu extrahieren.

Social-Engineering-Angriff: trickst EndnutzerInnen aus, damit sie vertrauliche Informationen preisgeben, die dann den Geräte- und Netzwerkzugriff ermöglichen.

BEISPIEL: Spoofing-Angriff, ermöglicht durch eine Phishing-E-Mail:

Ein/e EndnutzerIn fällt auf eine Phishing-E-Mail herein und gibt Zugangsdaten auf einer Spoofing-Webseite ein.

Die AngreiferInnen nutzen die gültigen Zugangsdaten, um sich remote Zugriff zum Netzwerk zu verschaffen.

Sie schleusen Daten über einen Webservice aus, verschlüsseln sie und fordern Lösegeld dafür.

Schutz für die moderne Arbeitsumgebung

In Bezug auf den Endpunktschutz sind Prävention, Erkennung und Reaktion sowie Recovery und Korrektur in verschiedenen Phasen über den gesamten Lebenszyklus eines Geräts erforderlich – von der Beschaffung und Fertigung der PCs über den Versand, die Bereitstellung und die Nutzung bis hin zur Stilllegung. Stellen Sie sich nur die Größe dieser kombinierten Angriffsfläche vor!

Die effektivste Cybersicherheitsstrategie plant für das Worst-Case-Szenario vor. Es wird davon ausgegangen, dass eine Sicherheitsverletzung möglich ist. Daher werden mehrere Schutzebenen implementiert, um den Angriff so schnell und so häufig wie möglich zu stoppen. Zudem minimieren die enthaltenen Korrekturfunktionen das Risiko eines Wiederholungsangriffs.

PRÄVENTION

Bieten Sie weniger Angriffsfläche, indem Sie für die Abwehr von Angriffen entwickelte Maßnahmen nutzen.

ERKENNUNG UND REAKTION

Gehen Sie stets von einer Sicherheitsverletzung aus und bleiben Sie wachsam.

RECOVERY UND KORREKTUR

Mindern Sie die Folgen eines Angriffs und kehren Sie zum normalen Geschäftsbetrieb zurück.

Schon gewusst?

Nur 33 %

der Unternehmen nutzen eine ganzheitliche End-to-End-Sicherheitsstrategie mit hardware- und softwarebasiertem Schutz.[3]

3. Dell Innovation Index, 2023.

Eine umfassende Lösung für sicheres Arbeiten – Tag für Tag

Da der PC das neue „Büro“ ist, wird eine umfassende Lösung benötigt, die Produktivität und Zusammenarbeit ermöglicht sowie gleichzeitig sicher, zuverlässig und persönlich ist. Zudem muss sich die hybride Belegschaft von heute eine **Cybersicherheitsroutine** aneignen.

Multifaktor-Authentifizierung (MFA), Zero-Trust-Prinzipien, Extended Detection and Response (XDR) sowie Antimalware und Patch-Updates in Verbindung mit hochwertiger Data Protection können NutzerInnen vor 99 % aller Angriffe schützen.*

Grundlagen einer Cybersicherheitsroutine

* www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Zukünftige Bedrohungen im Blick

Bei der Entwicklung innovativer Systeme achten Dell und Intel auf Risikominderung entlang ihrer Lieferketten, damit Geräte vom ersten Start an geschützt sind. Zudem ermöglicht Intel den Anbietern schon seit vielen Jahren Transparenz und Rückverfolgbarkeit der digitalen Lieferkette.

Intel® Transparent Supply Chain (Intel®TSC) stellt Trusted Computing Group (TCG)-Plattformzertifikate und Komponentendaten zur Unterstützung Intel basierter Plattformen über eine Cloud-API bereit, die der IT über das Intel®TSC-Webportal zur Verfügung steht.

In Verbindung mit der Dell Secured Component Verification (SCV)-Lösung sorgt dies für Kompatibilität und Interoperabilität, was die Sicherheit der digitalen Lieferkette für Intel-basierte Geräte verbessert.

Darüber hinaus setzen Dell, Microsoft und Intel auf Policies für die Beschaffung, den Zusammenbau und die Bereitstellung von Komponenten, um die Angriffsfläche zu minimieren, die Integrität der Geräte zu schützen und zum kontinuierlichen Schutz der Geräte beizutragen.

Hardwarebasierte Sicherheit in Form von Dell Trusted-Device-Technologien und Intel® Hardware Shield-Funktionen stärkt die Verteidigungsmechanismen der Geräte durch ein Framework aus Prävention, Erkennung und Reaktion. Außerdem erproben Sicherheitsteams in beiden Unternehmen die Produkte, um Sicherheitslücken aufzudecken, ehe AngreiferInnen es tun – sie entwickeln und veröffentlichen Patches, damit Sie und Ihre Teams geschützt bleiben.

Eine umfassende Lösung für sicheres Arbeiten – Tag für Tag

Windows 11 und Microsoft 365 Security: ein Fundament für sicheres Arbeiten – Tag für Tag.

Windows 11 bietet im Zusammenspiel mit Microsoft 365 Security eine umfassende Lösung, die für robuste Sicherheit bei der tagtäglichen Arbeit auf allen Ebenen eines Unternehmens sorgt. Im Folgenden wird erläutert, was diese Sicherheitskombination so herausragend macht.

Erhöhte Sicherheitsbaseline:
Durch moderne CPUs mit Funktionen wie virtualisierungsbasierter Sicherheit (VBS), hypervisorgeschützter Codeintegrität (HVCI) und Secure Boot setzt Windows 11 neue Maßstäbe in Sachen Sicherheit.
Weitere Informationen

Kennwortlose Authentifizierung:
Unter Windows 11 wird die kennwortlose Authentifizierung eingeführt, mit der das Risiko einer Gefährdung durch Kennwortangriffe reduziert wird.
Weitere Informationen

Multifaktor-Authentifizierung (MFA):
Windows 11 bietet robuste MFA-Funktionen, die über Kennwörter hinausgehen.
Weitere Informationen

Bereitschaft für hybrides Arbeiten:
Die modernen Sicherheitsfunktionen von Windows 11 sind für hybride Arbeitsumgebungen konzipiert.
Weitere Informationen

Microsoft Defender Antivirus:
Das in Windows 11 integrierte Microsoft Defender Antivirus bietet kontinuierlichen Schutz.
Weitere Informationen

Optimierte Sicherheitsfunktionen:
Windows 11 vereinfacht die Sicherheit, indem Funktionen standardmäßig aktiviert sind.
Weitere Informationen

Die Gestaltung einer sicheren Arbeitsumgebung

Für moderne Endpoint Security sind drei Elemente erforderlich:

1. **Softwaresicherheit:** Heutzutage befinden sich mehr NutzerInnen, Geräte und Daten außerhalb der Unternehmensnetzwerke als je zuvor. Softwaresicherheit schützt nicht nur die Geräte, sondern erweitert den Schutz auch auf Netzwerk- und Cloud-Umgebungen, in denen bösartige Aktivitäten häufig ihren Ursprung haben.

2. **Hardwaresicherheit:** Geräte müssen über integrierte Sicherheitsfunktionen verfügen. Das bezieht sich auf Hardware- und Firmwaresicherheit, die das Gerät während der Nutzung schützt. Zum Schutz der Arbeitsumgebung benötigen Sie integrierte Funktionen, die Ihnen Sichtbarkeit in und Kontrolle über das Gerät bieten.

3. **Sicherheit entlang der Lieferkette:** Geräte müssen sicher gebaut sein. Das heißt, mit Lieferanten zusammenzuarbeiten, die a) die Bedrohungslandschaft verstehen und b) diese Kenntnisse auf die sich entwickelnde Landschaft anwenden können. Der Schutz von Design, Entwicklung und Tests von PCs minimiert das Risiko für Sicherheitslücken in Produkten, und Lieferkettenkontrollen reduzieren das Risiko von Produktmanipulationen.

A Chief Technology Officer's Vision Board For 2024 And Beyond – Forbes-Artikel lesen

Darstellung der verschiedenen Sicherheitsebenen

(Repräsentative Beispiele der aufgeführten Sicherheitsmaßnahmen)

Softwaresicherheit

- Virenschutz der nächsten Generation (NGAV)
- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Data Protection für die Cloud
- Netzwerkschutz
- Automatische Fehlerkorrektur

Hardware-/Firmwaresicherheit

- Überprüfung zur Startzeit
- Überprüfung zur Laufzeit
- Nutzerauthentifizierung
- Sicherheitsbenachrichtigungen und Warnmeldungen/Telemetrie

Sicherheit entlang der Lieferkette

- Sichere Entwicklungspraktiken
- Sichere Lieferkettenpraktiken
- Komponentenprüfungen
- Manipulationssichere Verpackung

Windows 11 und Microsoft 365 Security

Windows 11 und Microsoft 365 Security schaffen eine vertrauenswürdige Umgebung, in der die Produktivität gesteigert wird, ohne Abstriche bei der Sicherheit zu machen – von grundlegenden Aufgaben bis hin zu strategischer Entscheidungsfindung.

Copilot in Windows und Copilot für Microsoft 365 tragen wesentlich dazu bei, die Produktivität und Sicherheit für NutzerInnen zu erhöhen.

Der Beitrag von Copilot in Microsoft 365 und Windows zu einer sicheren PC-Arbeitsumgebung
Copilot orchestriert Aufgaben, liefert präzise Antworten und ermöglicht es NutzerInnen, sich auf strategische Tätigkeiten zu konzentrieren.

Geräte auf spezielle Arbeitsanforderungen abstimmen
Copilot vereinfacht die Gerätekonfiguration, indem es Einstellungen anpasst, wesentliche Software installiert und dabei hilft, spezifische Anforderungen zu erfüllen, sodass Effizienz und Effektivität sichergestellt werden.

Management, Upgrades und Nutzung von Betriebssystemen leicht gemacht
Copilot bietet Unterstützung für das Management von Betriebssystemaufgaben.

Estate-Gerätemanagement

Endpoint Security gegen Cyberangriffe
Copilot trägt zur allgemeinen Sicherheit bei, indem es Sicherheitsrichtlinien für Microsoft 365 und Windows 11 einhält.

Anwendungen für die Zusammenarbeit für Information und Frontline Worker
Windows Copilot und Microsoft 365 Copilot verbessern die Zusammenarbeit und Produktivität von Information und Frontline Workers durch intelligente Unterstützung und nahtlose Integration über Geräte hinweg.

Zusammenfassend gesagt, trägt Microsoft Copilot zu einer sicheren Arbeitsumgebung bei, indem es Abläufe optimiert, die Sicherheit erhöht und eine bessere Zusammenarbeit zwischen verschiedenen Rollen und Geräten ermöglicht.

Blog lesen

Unser Ansatz: Dell Trusted Workspace

Dell ist Sicherheits- und IT-Partner für Unternehmen weltweit. Im Gegensatz zu Punktlösungen legt Dell den Schwerpunkt auf die Sicherheitsergebnisse. Wir haben eine Suite mit Lösungen entwickelt, die Kill Chains unterbrechen und so Ihre Ausfallsicherheit bei Cyberangriffen erhöhen.

Dell Trusted Workspace umfasst Folgendes:

- Einzigartiger **Hardware- und Firmwareschutz** – das macht Dell zum Anbieter der branchenweit sichersten PCs[4] *(eingebaute und integrierte Sicherheit)*
- Partnernetzwerk mit **branchenführender Software** für Advanced Threat Protection – für Geräte sowie Netzwerk- und Cloud-Umgebungen *(zusätzliche Sicherheit)*

Zusätzliche Softwaresicherheit durch Partnernetzwerk

- **Dell SafeGuard and Response: CrowdStrike, Carbon Black** und **Secureworks** sorgen für die Erkennung, Abwehr und Korrektur von Bedrohungen.
- **Dell SafeData: Netskope** sorgt für Sichtbarkeit, Monitoring und die Verhinderung von Datenverlusten bei cloudbasierten Apps. **Absolute** aktiviert die automatische Fehlerkorrektur für Apps und Netzwerke.

Integrierte Hardware- und Firmwaresicherheit in den branchenweit sichersten PCs[4]

Beispielfunktionen für den Schutz während der Gerätenutzung:

- **Dell SafeBIOS** fängt bösartige Aktivitäten mithilfe von Off-Host BIOS Verification* und Indicators of Attack* ab, bevor sie den PC schädigen können.
- **Dell SafeID** schützt die Nutzerzugangsdaten auf einem dedizierten Chip.*
- **Firmwareverifizierung unabhängig vom Host** schützt die Integrität von Firmware mit besonderen Berechtigungen.*
- Mit der **Dell Trusted-Device-Software** integriert Dell die Gerätetelemetrie in branchenführende Software, um die Sicherheit der ganzen Flotte zu verbessern.*
- **Intel® Hardware Shield** hilft, Angriffe auf Firmware zu verhindern und Anwendungen vor Angriffen zu schützen, die über das BIOS ausgeführt werden.

Eingebaute Lieferkettensicherheit sorgt dafür, dass PCs ab dem ersten Start geschützt sind.

- **Dell SafeSupply Chain**-Add-ons wie Dell Secured Component Verification bieten eine zusätzliche Absicherung für die Produktintegrität.

* Nur bei Dell

4. Basierend auf einer internen Analyse von Dell, September 2023. Gilt für PCs mit Intel Prozessoren. Nicht alle Funktionen sind bei jedem PC verfügbar. Einige Funktionen müssen zusätzlich erworben werden.

Eine umfassende Lösung von Dell, Intel und Microsoft

Mit sowohl hardware- als auch softwarebasierten Gegenmaßnahmen verkleinern Sie die Angriffsfläche durch eine Abwehr, die gängige Angriffe verhindert.

Erkennungs- und Reaktionsfunktionen fangen versteckte Angriffe ab, die sonst vielleicht „durchkommen“ würden.

Bei einem Angriff auf die Lieferkette (wie auf Seite 4 beschrieben): Bei einer Zusammenarbeit mit Dell können präventive Maßnahmen, wie z. B. **sichere Lieferkettenpraktiken**, einen Angriff frühzeitig in der Kill Chain stoppen. Falls ein Angriff „durchkommt“, greifen zusätzliche Gegenmaßnahmen, wie z. B. **SCV** (Secured Component Verification).

Bei einem Social-Engineering-Angriff: Selbst wenn es den AngreiferInnen gelingt, EndnutzerInnen auszutricksen, damit sie gültige Zugangsdaten preisgeben, kann eine **hardwarebasierte Nutzerverifizierung wie SafeID** den Angriff stoppen und weiteren Zugriff verwehren.

Sicherheitssoftware wie **Next-Gen Secure Web Gateway** bietet eine weitere Ebene für den Monitoringschutz.

Abwehren eines Angriffs auf die Hardwarelieferkette, ermöglicht durch die Manipulation einer Komponente

Die AngreiferInnen fangen einen PC-Versand ab und tauschen die Festplatten.

- **Sichere Lieferkettenpraktiken**
- Manipulationssichere Verpackung
- Türschlösser

Die IT stellt die kompromittierten Geräte im Unternehmen bereit.

- Sichere Komponentenverifizierung (Secured Component Verification, SCV)
- Überprüfung zur Laufzeit

Die AngreiferInnen installieren Malware, um die Zugangsdaten während des Anmeldevorgangs der NutzerInnen zu extrahieren.

- Cloud Access Security Broker
- Next Generation Secure Web Gateway (NG-SWG)

Abwehren eines Social-Engineering-Angriffs, ermöglicht durch eine Phishing-E-Mail

Ein/e EndnutzerIn fällt auf eine Phishing-E-Mail herein und gibt Zugangsdaten auf einer Spoofing-Webseite ein.

- NGAV
- EDR
- XDR

Die AngreiferInnen nutzen die gültigen Zugangsdaten, um sich remote Zugriff zum Netzwerk zu verschaffen.

- **Multifaktor-Authentifizierung mit SafeID**
- Zero Trust Network Access

Sie schleusen Daten über einen Webservice aus, verschlüsseln sie und fordern Lösegeld dafür.

- Next Generation Secure Web Gateway + Verhaltensanalysen von Nutzerentitäten

Das Zero-Trust-Sicherheitsmodell

Windows 11 unterstützt das Zero-Trust-Sicherheitsmodell. Dieses Konzept basiert auf drei Säulen:

1 **Kein Zugriff ohne Nachweis von Sicherheit und Integrität:**
Windows 11 arbeitet nach dem Prinzip, dass kein/e NutzerIn und kein Gerät auf irgendetwas zugreifen darf, bis seine/ihre Sicherheit und Integrität bestätigt wurden. Um sicherzustellen, dass ein Computer nicht manipuliert wurde, setzt Windows 11 auf eine explizite Verifizierung – Authentifizierung und Autorisierung – anhand aller verfügbaren Datenpunkte. Dazu gehören Nutzeridentität, Standort, Gerätestatus, Service oder Workload, Datenklassifizierung und Anomalitäten.

2 **Zugriff mit geringsten Rechten:**
Windows 11 ermöglicht die Verwendung des Zugriffs mit geringsten Rechten. Da der Nutzerzugriff durch risikobasierte, anpassungsfähige Just-in-Time- und Just-Enough-Access-Policies beschränkt ist, werden sowohl Daten als auch die Produktivität geschützt.

3 **Ausgehen von einer Sicherheitsverletzung:**
In diesem Szenario wird davon ausgegangen, dass sich HackerInnen bereits Zugang zum System verschafft haben. Die Strategie besteht darin, so zu agieren, dass der betroffene Radius und der Segmentzugriff minimiert werden. Die End-to-End-Verschlüsselung wird verifiziert und es werden Analysen durchgeführt, um Sichtbarkeit zu erhalten, die Bedrohungserkennung voranzubringen und Abwehrmechanismen zu verbessern.

Dieses Sicherheitsmodell sorgt für einen robusten Schutz auf allen Ebenen, was allen zugutekommt, von Frontline-MitarbeiterInnen bis hin zur Geschäftsleitung.

Windows 11 Pro:
Basis für sichere hybride Arbeitsumgebungen

Windows 11 Pro wurde speziell für hybride Arbeitsumgebungen entwickelt und bietet erweiterte Sicherheitsfunktionen sowie Schutz vor Angriffen. Dell Geräte mit Intel® Core™ Ultra Prozessoren, die Windows 11 ausführen, stellen die sicherste Option am Markt dar und verfügen über integrierte hardwarebasierte Sicherheit. Windows 11 bietet vorab aktivierte Sicherheitskomponenten und ermöglicht so beispiellose Produktivität und Sicherheit.

In Verbindung mit Microsoft 365 sorgen Dell Trusted-Devices für umfassende Unternehmenssicherheit, ohne dass Eingriffe vor Ort erforderlich sind. Microsoft 365 ermöglicht Kosteneinsparungen, robuste Sicherheit, verbesserte Produktivität und nahtlose Integration. Mit Dell Technologies erhalten Sie Zugang zu einem spezialisierten Serviceteam, umfassendem Einrichtungs- und Installationssupport sowie Remotemanagement und Unterstützung rund um die Uhr.

Weitere Informationen zu Sicherheitsfunktionen von Windows 11

Video zu Sicherheitsfunktionen von Windows 11 ansehen

Wichtigste Erkenntnisse

Sicherheitsverletzungen sind unvermeidbar.
Effektive Endpoint Security geht immer vom Worst-Case-Szenario aus und konzentriert sich darauf, Kill Chains zu stoppen, wo immer sie auftreten – vom Gerät über das Netzwerk bis zu Cloud.

Keine Lösung blockiert 100 % der Angriffe.
Eine Kombination aus hardware- und softwarebasierten Gegenmaßnahmen bietet die bestmögliche Abwehr.

Sie sind immer nur so sicher wie Ihre Lieferanten.
Fordern Sie Ihre Lieferanten auf, ihre Sicherheitsmaßnahmen darzulegen.

Weitere Informationen:

Kontaktieren Sie uns:
Global.Security.Sales@Dell.com

Besuchen Sie uns unter:
Dell.com/Endpoint-Security

Folgen Sie uns:
LinkedIn @DellTechnologies
X @DellTech

Ihr nächster Schritt

Das Thema Sicherheit ist für Unternehmen jeder Größe eine echte Herausforderung. **Dank umfassender Schutzmaßnahmen auf Hardware- und Softwareebene von Intel und Microsoft, die von Dell vereint werden, entsteht eine modernisierte Endpoint-Security-Lösung.**

Dell Trusted Workspace trägt zum Schutz von Endpunkten bei, damit Sie eine moderne, Zero-Trust-fähige IT-Umgebung aufbauen können. Verkleinern Sie die Angriffsfläche mit einem umfassenden Portfolio an Hardware- und Softwareschutz, exklusiv von Dell. Unser rundum koordinierter, abwehrbasierter Ansatz entschärft Bedrohungen, indem integrierte Schutzmaßnahmen mit kontinuierlicher Wachsamkeit kombiniert werden. Unsere Sicherheitslösungen wurden für die cloudbasierte Welt von heute konzipiert und sorgen für Produktivität seitens der EndnutzerInnen und eine starke IT.

DELL Technologies

intel. Accelerate AI with Intel®

Windows 11