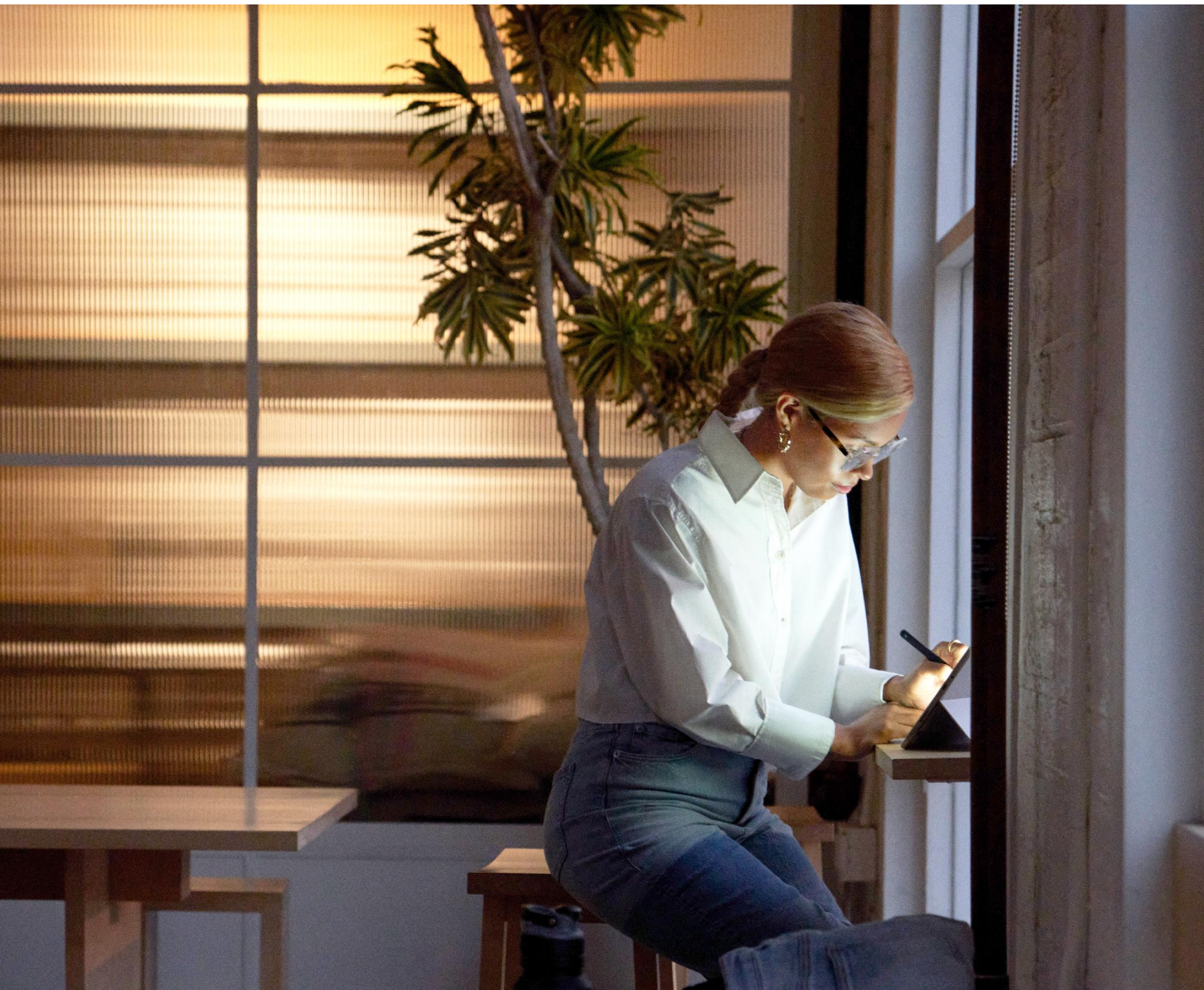
Microsoft Surface

Mit Bedacht wählen: Wie die Geräteauswahl über den Erfolg oder Misserfolg Ihres Cyberresilienzplans entscheidet



Was bedeutet es, cyberresilient zu sein?

Fast jedes Unternehmen, vom Café um die Ecke bis zum Weltkonzern, ist heute auf Daten, Analytics, Automatisierung und digitale Technologien angewiesen. Diese Abhängigkeit in Verbindung mit einer dezentral arbeitenden Belegschaft hat das Risiko und die Kosten von Cyberangriffen in einem Ausmaß erhöht, das von lokalen bis hin zu globalen Auswirkungen reicht.

Da Angriffe immer häufiger und komplexer werden, müssen erfolgreiche Sicherheitsverantwortliche jetzt mehr als nur Prävention betreiben. Unter Cyberresilienz versteht man die Fähigkeit eines Unternehmens, schnell zu reagieren und sich von einem negativen Ereignis gut zu erholen, um die finanziellen Auswirkungen von Sicherheitsschwachstellen zu minimieren. Resilienz kann den Unterschied ausmachen zwischen einem Rückschlag oder einem Schritt nach vorn.

5-mal mehr Cyberattacken auf remote verwaltete Geräte zwischen Mai 2021 und Mai 2022.[1]

4,24 Mio. USD kostete 2022 eine Datenschutzverletzung im weltweiten Durchschnitt.[1]

[1]Microsoft, Microsoft Digital Defense Report 2022, 2022.

(Fortsetzung) Was bedeutet es, cyberresilient zu sein?

Wie ist das möglich? Von Großkonzernen über mittelständische Firmen bis hin zu Kleinstbetrieben: Es gibt wichtige Grundsätze, die jedes Unternehmen anwenden kann, um gestärkt aus einer Krise hervorzukommen. Dazu ist eine pragmatische Sichtweise auf die Cybersicherheit erforderlich, wobei davon ausgegangen wird, dass Sicherheitsverletzungen unvermeidlich sind. Mit anderen Worten: Sie müssen davon ausgehen, dass eine Kompromittierung vorliegt.

Eine solche Annahme ist eine deutliche Abkehr von der traditionellen Sicherheitsmentalität. Bislang glaubten IT-Fachleute, sie könnten ein sicheres Netzwerk mit einem geschützten aufbauen, indem sie alle Geschäftsvorgänge auf das Netzwerk beschränken und gleichzeitig die Geräte der Endbenutzer*innen streng kontrollieren.

Dieser traditionelle Ansatz vernachlässigt jedoch die Anforderungen moderner Arbeitsumgebungen, sich ändernder Geschäftsmodelle, neuer Technologien und sich wandelnder Sicherheitsbedrohungen. Um die Resilienz zu stärken, bedarf es Zero Trust, einer partnerschaftlichen Zusammenarbeit zwischen Stakeholdern, IT-Führungskräften und Sicherheitsexpert*innen sowie den Einsatz moderner Technologien, die den Schutz verbessern.

Bis 2026 werden **50 %** der Führungskräfte im Top-Management Arbeitsverträge haben, in denen risikobezogene Leistungsanforderungen festgelegt sind.[1]

Bis 2025 werden **60 %** der Unternehmen das Cybersicherheitsrisiko als primäres Kriterium für Geschäftsabschlüsse und die Vergabe von Aufträgen an Dritte zugrunde legen.[1]

[1]Gartner-Pressemitteilung, „Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23", 21. Juni 2022. https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

In zwei Schritten zu mehr Cyberresilienz

01 Grundlegende Maßnahmen umsetzen

Die meisten Cyberangriffe lassen sich durch einfache Maßnahmen wie die Ausmusterung veralteter Anwendungen, Geräte und Infrastrukturen verhindern. Zudem wird empfohlen, manuelle Prozesse zu automatisieren, die Multi-Faktor-Authentifizierung (MFA) zu aktivieren, Zero Trust-Prinzipien zu übernehmen und modernen Malware-Schutz einzusetzen.

Regelmäßige Firmware- und Software-Updates beseitigen fortlaufend Sicherheitslücken. Firmware-Angriffe stellen eines der größten Risiken für Unternehmen dar. Hierbei verschaffen sich böswillige Akteure über Geräte (von Laptops über Drucker bis hin zu Routern und mehr) unentdeckt uneingeschränkten Zugang zu Ihrem Netzwerk.

Ein wichtiger erster Schritt beim Aufbau von Cyberresilienz besteht darin, jene Benutzerendpunkte zu identifizieren, deren Firmware zugänglich ist.

---

98 % der Angriffe lassen sich durch grundlegende Hygienemaßnahmen verhindern.[1]

45 % der Sicherheitsfachleute nennen E-Mail-Programme und Tools für die Zusammenarbeit als die Bereiche in ihrem Unternehmen, die am anfälligsten für Angriffe sind.[2]

[1]Microsoft, Microsoft Digital Defense Report 2022, 2022.
[2]Microsoft, Cyber Resilience, 2022.

Schlüsselkomponenten der Cyberresilienz

Schützen und abwehren

Alle guten Resilienzstrategien beruhen auf dem Schutz von Systemen, Anwendungen und Daten. Gewähren Sie nur autorisierten Benutzer*innen, die Kunden-, Mitarbeiter- und Geschäftsdaten benötigen, Zugriff Prüfen Sie außerdem Anwendungen und Endpunktgeräte auf Schwachstellen, die überall – vom Chip bis zur Cloud – lauern können.

Ermitteln und überprüfen

Cyberangriffe häufen sich und werden immer ausgeklügelter. Daher ist es wichtig, Geräte und Software mithilfe von Diagnosetools kontinuierlich auf Anomalien zu überwachen. Automatisierung kann hierbei hilfreich sein, wenn es darum geht, Systemreaktionen bei bestimmten Bedrohungen auszulösen und jene Bedrohungen zu priorisieren, die von einem Teammitglied eingehender geprüft werden sollen.

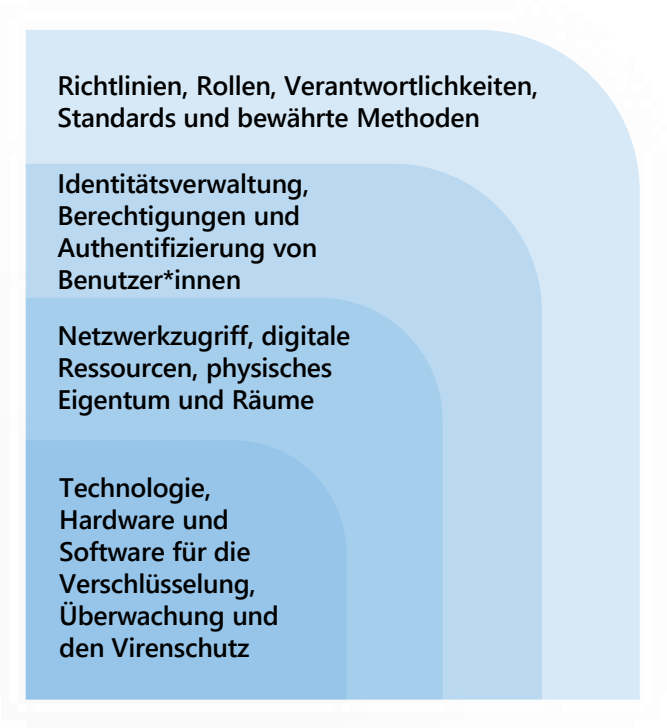
Erholen

Angriffe sind unvermeidlich. Wer das akzeptiert, kann für kürzere Betriebsstörungen und eine effiziente Wiederherstellung planen, und zwar mit cyberresilienten Geräten.

02 In störungsresistente Technologie investieren

Sicherheitsverantwortliche investieren massiv in die Softwaresicherheit. Firewalls, Datenverschlüsselung, Angriffserkennung und Angriffsschutz stehen dabei ganz oben auf der Liste. Die Hardware-Anfälligkeit zu vernachlässigen, kann jedoch alle Bemühungen zunichtemachen.

Eine typische Sicherheitsinfrastruktur umfasst mehrere Ebenen, die zusammenarbeiten, um die Firmenressourcen, Geschäftsdaten und den Betrieb zu schützen.



Eine Kompromittierung auf der Hardwareebene durch ein Notebook, Tablet, Smartphone oder IoT-Gerät breitet sich aus und kompromittiert andere Ebenen, um die Daten und Netzwerke zu erreichen, die durch die Hardware eigentlich geschützt werden sollen.

Die Zusammenarbeit mit Technologie-Entscheidungsträger*innen bei der Auswahl des richtigen Geräts ist eine wichtige Voraussetzung für Ihren Cyberresilienzplan. Faktoren, wie die auf die Nutzung abgestimmte Leistung, Skalierbarkeit, Kompatibilität, Zuverlässigkeit sowie die Sicherheit des Geräts selbst spielen, dabei eine Rolle.

Schlüsselkomponenten einer cyberresilienten Infrastruktur

- Erstellen Sie einen Firmware-Schutzplan, und achten Sie auf Firmware-, UEFI- und Betriebssystem-Updates, die zusätzlichen Schutz vor neuen Bedrohungen bieten können.
- Beschleunigen Sie die Automatisierung manueller Aufgaben wie Remote-Updates und Geräteaktivierung, sodass den IT-Teams mehr Zeit für andere Tätigkeiten bleibt.
- Erstellen Sie einen Zeitplan zum Aufspielen von UEFI-, Firmware- und Sicherheitsupdates.
- Aktivieren Sie die MFA für alle Anwender*innen, und implementieren Sie eine Strategie für den bedingten Zugriff.
- Setzen Sie auf biometrische Scans (z. B. Windows Hello for Business), um die Abhängigkeit von Zugangscodes, Chipkarten und Passwörtern zu reduzieren.
- Nutzen Sie Geräte, die als Secured-Core-PCs gelten, oder konfigurieren Sie Ihre Geräte so, dass sie ähnliche Anforderungen erfüllen.
- Beheben Sie Schwachstellen in Endpunktgeräten, indem Sie ungenutzte Funktionen wie Bluetooth oder Videokameras deaktivieren.

Auswahl cyber-resilienter Geräte

- Informieren Sie sich über bewährte Methoden und Standards für die Gerätesicherheit in Ihrer Branche.
- Bewerten Sie Ihren aktuellen Gerätebestand, und identifizieren Sie Lücken oder Risiken in Bezug auf Funktionalität, Alter, Version oder Sicherheit.
- Vergleichen Sie verschiedene Geräte im Hinblick auf Funktionsumfang, Vorteile, Nachteile, Tests und Bewertungen.
- Lassen Sie sich bei der Geräteauswahl von Expert*innen oder Anbietern beraten.
- Testen und bewerten Sie die Leistung und Sicherheit der von Ihnen ausgewählten Geräte vor deren Einsatz in Ihrem Unternehmen.
- Überwachen und warten Sie Ihre Geräte regelmäßig, um sicherzustellen, dass sie ordnungsgemäß funktionieren.

Geräte auf dem neuesten Stand halten

IT-Teams können zwar Geräte ständig testen und deren Verwendungszweck einschränken, doch indem die Geräte-Firmware auf dem neuesten Stand gehalten wird, verringert sich das Risiko, und die IT-Teams können sich auf Resilienz und Wachstum konzentrieren, anstatt auf Verteidigung und Reparatur.

Neben Firmware-Angriffen nehmen auch Attacken auf remote verwaltete Geräte zu. Zu solchen Geräten gehören Laptops, Kameras und smarte Konferenzraumtechnologie, deren offenliegende Ports von Hackern ausgenutzt werden. Eine aktuelle Studie ergab, dass 46 % der IoT-/OT-Angriffe von remote verwalteten Geräten ausgingen.[1]

[1]Microsoft Security Insider, Unpatched and Exposed, The Unique Security Risk of IoT/OT Devices, 2022.

Wählen Sie einen Partner, der Sie bei der Entwicklung einer Cyber-Resilienzstrategie unterstützt

In einer Welt voller komplexer IT-Herausforderungen kann die Wahl des richtigen IT-Partners dazu beitragen, Unternehmen zu schützen und sie auf den Neustart vorzubereiten. Ein guter IT-Partner empfiehlt die für das jeweilige Unternehmen am besten geeigneten Hardware-, Software- und Sicherheitslösungen und erspart das lästige Hin und Her mit mehreren Anbietern oder Lösungen. Ein wertvoller IT-Partner verfügt über das Wissen und die Erfahrung, um bei der Entwicklung und Umsetzung eines umfassenden Cyberresilienzplans zu helfen, der sich an das wachsende Unternehmen anpasst. Letztendlich sollte ein IT-Partner im Interesse seiner Kunden agieren und ihnen zum Erfolg verhelfen.

Gemeinsam mit unseren Partnern hat Microsoft die Surface-Geräte darauf ausgelegt, das Bedrohungsrisiko für Firmware, Betriebssystem und Cloud-Anwendungen zu minimieren. Zero Trust ist von Grund auf integriert. Deshalb können Sicherheitsverantwortliche und IT-Entscheidungsträger*innen getrost Ressourcen in Strategien und Technologien investieren, die zukünftige Angriffe verhindern, anstatt sich ständig gegen den gegenwärtigen Ansturm von Cyberattacken zu verteidigen.

Finden Sie einen Microsoft-Partner: Autorisierte Microsoft-Händler für Surface for Business

Wie Microsoft Surface die Cyberresilienz stärkt

Microsoft Surface-Geräte erleichtern grundlegende Maßnahmen zur Sicherheitshygiene, wobei jede Ebene von Microsoft gepflegt wird, von der Firmware über das Betriebssystem bis hin zur Cloud. Surface-Geräte, Windows 11 und Microsoft 365[1] stärken mit einem Zero Trust-Ansatz bei Sicherheit und Risikomanagement die Resilienz von Unternehmen, ohne dass Innovationen oder Produktivität darunter leiden.

Als wir Surface entwickelten, haben wir uns darüber Gedanken gemacht, inwiefern Cyberangriffe Geräte und Benutzer*innen gefährden können. Sicherheit ist am effektivsten, wenn sie von Grund auf integriert ist; und genau das haben wir getan. So lassen sich die am häufigsten gefährdeten Bereiche schützen. Surface-Geräte bieten Schutz vom Chip bis zur Cloud. Die integrierte Lösung von Microsoft schützt Ihr Geschäft. Auf Surface ist also Verlass. Sehen wir uns nun genauer an, wie Microsoft Surface die Cyberresilienz stärkt.

Wer als Unternehmen Surface einsetzt, verzeichnet bis zu 34 % weniger Sicherheitsvorfälle und spart Zeit bei der Reaktion auf Sicherheitsvorfälle.[2]

*Nur bei Microsoft Surface.
**Customer Replaceable Units (CRUs) sind Komponenten, die Sie über Surface Commercial Authorized Device Reseller erwerben können. Die Komponenten können vor Ort von einer technischen Fachkraft unter Beachtung des Servicehandbuchs von Microsoft ausgetauscht werden. Beim Öffnen und/oder Reparieren Ihres Geräts besteht die Gefahr von Stromschlägen, Bränden, Verletzungen und anderen Gefahren. Seien Sie vorsichtig, wenn Sie Reparaturen selbst durchführen. Während der Reparatur verursachte Geräteschäden sind nicht durch Microsofts Hardwaregarantie oder Schutzpläne abgedeckt. Die Komponenten sind kurz nach der Markteinführung verfügbar; der Verfügbarkeitszeitpunkt variiert je nach Komponente und Markt.
[1]Für einige Funktionen ist eine Softwarelizenz erforderlich. Separat erhältlich.
[2]Whitepaper zum Thema Business Value, im Auftrag von Microsoft, September 2022 | Dok.-nr. #US49453722 Befragungen und Interviews im Rahmen der IDC-Studie fanden zwischen Dezember 2021 und Februar 2022 statt. Alle Befragten waren IT-Entscheidungsträger*innen in großen Unternehmen (250–5000 Beschäftige) und repräsentierten Organisationen aus den USA, Australien, Indien, Spanien, Frankreich, Großbritannien, Neuseeland und Deutschland. Die Kosten- und Einsparungsergebnisse basieren auf durchschnittlichen Kosten- und Zeitschätzungen der Befragten. Tatsächliche Kosten und Einsparungen können je nach spezifischem Gerätemix und Bereitstellung variieren. Die ausführliche Studie finden Sie hier.

Cyberresilienz bei der Hardware, bei der Zusammenarbeit und in der Cloud erreichen

„Microsoft bietet alle Dienste und Abwehrmaßnahmen, die wir für uns und unsere Kunden benötigen, auf ein und derselben Plattform an."

NIP Group

Microsoft Surface kann dazu beitragen, Sicherheitslücken zu schließen, weil es Sicherheitsteams, Führungskräfte und Mitarbeitende unterstützt. Die auf Sicherheit ausgelegten Surface-Geräte bieten in Kombination mit Windows 11 und Microsoft 365* eine integrierte Lösung samt Schutzebenen und Remote-Geräteverwaltung, die von der Hardware über die Firmware bis zur Cloud reicht.

Hardware- und Softwaresicherheitsfunktionen sind bei Windows 11 ab Werk integriert und bieten Resilienz sowie proaktiven Schutz gegen sich ständig wandelnde Bedrohungen.

*Für einige Funktionen ist eine Softwarelizenz erforderlich. Separat erhältlich.

„Secured-Core PC ist ein Versuch, ‚die beste Umgebung der Welt' zu schaffen. Ich glaube, dass wir eine solche Umgebung erfolgreich bereitgestellt haben, indem wir die neuesten Technologien, darunter Microsoft 365, mit unseren eigenen kombiniert haben."

NTT Communications Corporation

Konzipiert für Sicherheit

Unser Sicherheitsansatz beginnt bei der Hardware. Surface schützt Daten, indem es sie schon beim Hochfahren des Geräts verschlüsselt. Ein **Trusted Platform Module 2.0** (TPM 2.0) fungiert als sicherer Tresor. Darin gespeichert sind Passwörter, PINs und Zertifikate. TPM 2.0 schützt die Hardware vor Manipulationen und beschränkt den Zugriff auf autorisierte Personen. Beim Hochfahren wird die Echtheit des Firmware-Codes geprüft, um sicherzustellen, dass das System keinen bösartigen Code ausführt.

Die passwortlose, sichere Anmeldung per **Windows Hello for Business** bietet ein Höchstmaß an biometrischer Sicherheit. Infrarotkamerasensoren verbessern die Gesichtserkennung. Biometrische Merkmale lassen sich nur schwer replizieren, so ist sichergestellt, dass nur autorisierte Nutzer*innen auf das Gerät zugreifen können.

Viele Surface-Geräte verfügen über entnehmbare SSDs[1] und bieten so mehr Schutz für auf dem Gerät gespeicherte vertrauliche Daten.

Microsoft wurde 2022 im Gartner® Magic Quadrant™ als führender Anbieter von Tools für die einheitliche Endpunktverwaltung ausgezeichnet.[2]

Unternehmen, die Surface einsetzen, konnten den Zeitaufwand der IT-Angestellten für die laufende Wartung um 40 % reduzieren.[3]

Vertrauensfördernd

Surface Management Portal ist in **Microsoft Intune*** integriert und bietet eine dedizierte, zentralisierte, cloudbasierte Endpunktverwaltungslösung. Mit dem Surface Management Portal lassen sich die Herausforderungen bei der bedarfsgerechten Verwaltung und Konfiguration von Benutzer*innen, Anwendungen und Geräten meistern. Microsoft Intune* übernimmt die Verwaltung mobiler Anwendungen und mobiler Geräte.

---

*Für einige Funktionen ist eine Softwarelizenz erforderlich. Separat erhältlich.
[1]Customer Replaceable Units (CRUs) sind Komponenten, die Sie über Surface Commercial Authorized Device Reseller erwerben können. Die Komponenten können vor Ort von einer technischen Fachkraft unter Beachtung des Servicehandbuchs von Microsoft ausgetauscht werden. Beim Öffnen und/oder Reparieren Ihres Geräts besteht die Gefahr von Stromschlägen, Bränden, Verletzungen und anderen Gefahren. Seien Sie vorsichtig, wenn Sie Reparaturen selbst durchführen. Während der Reparatur verursachte Geräteschäden sind nicht durch Microsofts Hardwaregarantie oder Schutzpläne abgedeckt. Die Komponenten sind kurz nach der Markteinführung verfügbar; der Verfügbarkeitszeitpunkt variiert je nach Komponente und Markt.
[2]Gartner, Magic Quadrant for Unified Endpoint Management Tools, Tom Cipolla, Dan Wilson, u. a., 1. August 2022. GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seinen Tochtergesellschaften in den USA und international, und MAGIC QUADRANT ist eine eingetragene Marke von Gartner, Inc. und/oder seinen Tochtergesellschaften. Beide Marken werden in diesem Dokument mit Genehmigung verwendet. Alle Rechte vorbehalten. Gartner empfiehlt weder die in dieser Marktbetrachtung abgebildeten Lösungsanbieter, Produkte oder Dienstleistungen, noch wird Technologienutzenden geraten, ausschließlich die am höchsten bewerteten und am besten ausgezeichneten Lösungsanbieter auszuwählen. Die Gartner-Marktbetrachtungen beruhen auf den Meinungen der Gartner-Forschungsorganisation und sollten nicht als Sachverhalt aufgefasst werden. Gartner übernimmt keinerlei Garantien, weder ausdrücklich noch impliziert, für diese Recherchen, einschließlich aller Garantien für die allgemeine Gebrauchstauglichkeit oder die Eignung für einen bestimmten Zweck.
[3]Whitepaper zum Thema Business Value, im Auftrag von Microsoft, September 2022 | Dok.-nr. #US49453722 Befragungen und Interviews im Rahmen der IDC-Studie fanden zwischen Dezember 2021 und Februar 2022 statt. Alle Befragten waren IT-Entscheidungsträger*innen in großen Unternehmen (250–5000 Beschäftige) und repräsentierten Organisationen aus den USA, Australien, Indien, Spanien, Frankreich, Großbritannien, Neuseeland und Deutschland. Die Kosten- und Einsparungsergebnisse basieren auf durchschnittlichen Kosten- und Zeitschätzungen, die direkt von den Befragten zur Verfügung gestellt wurden. Tatsächliche Kosten und Einsparungen können je nach spezifischem Gerätemix und Bereitstellung variieren. Die ausführliche Studie finden Sie hier.

Windows Update verwaltet das Roll-out und die Aktualisierung von Firmware, Software und Treibern. Ein lückenloser Schutz stellt sicher, dass nur genehmigte Inhalte installiert sind.

Die Möglichkeit, die Gerätesicherheit remote zu verwalten, kann Ihrem IT-Team viel Zeit ersparen, da die Wahrscheinlichkeit von Firmware- oder Ransomware-Angriffen verringert wird und Probleme behoben werden können, bevor sie sich ausweiten.

Im Zusammenspiel mit Microsoft Intune* spart **Windows Autopilot** mehr Zeit, weil es neue Geräte mit den erforderlichen Sicherheitseinstellungen und Richtlinien vorkonfiguriert und so die Remote-Bereitstellung vereinfacht.

„Die biometrische Authentifizierung per Gesichtserkennung durch Windows Hello, wie wir sie beim Surface erleben, ist absolut marktführend."

Mashreq

Gesperrte Firmware

Surface-Geräte blockieren Bedrohungen proaktiv, indem sie das Unified Extensible Firmware Interface (UEFI), einen wichtigen externen Zugangspunkt zur Firmware, sperren. Das von Microsoft entwickelte UEFI ist über Windows Update zugänglich, wodurch das Risiko eines externen Zugriffs auf die Firmware sinkt.

Microsofts UEFI ermöglicht zusammen mit dem **Device Firmware Configuration Interface (DFCI)** eine detailliertere Steuerung der Firmware durch Microsoft Intune.*

DFCI verkleinert die Angriffsfläche, indem es nicht benötigte Hardwarekomponenten deaktiviert und die Abhängigkeit vom lokalen UEFI-Passwort beseitigt. DFCI bietet die Möglichkeit, Boot-Optionen zu sperren, um zu verhindern, dass Nutzer*innen ein anderes Betriebssystem booten. Im Hintergrund ablaufende Sicherheitsupdates bieten kontinuierlich Schutz vor den neuesten Bedrohungen.

---

34 % weniger Sicherheitsvorfälle bei Surface-Geräten.[2]

30 % Zeitersparnis für IT-Angestellte bei Sicherheitsvorfällen dank Surface-Geräten.[2]

---

*Für einige Funktionen ist eine Softwarelizenz erforderlich. Separat erhältlich.
[1]Surface Go und Surface Go 2 verwenden ein UEFI eines Drittanbieters und unterstützen DFCI nicht. Einzelheiten zum Microsoft-Schutz für Surface Go und Go 2 finden Sie unter https://www.microsoft.com/en-us/surface/business/surface-go-2.
[2]Whitepaper zum Thema Business Value, im Auftrag von Microsoft, September 2022 | Dok.-nr. #US49453722 Befragungen und Interviews im Rahmen der IDC-Studie fanden zwischen Dezember 2021 und Februar 2022 statt. Alle Befragten waren IT-Entscheidungsträger*innen in großen Unternehmen (250–5000 Beschäftige) und repräsentierten Organisationen aus den USA, Australien, Indien, Spanien, Frankreich, Großbritannien, Neuseeland und Deutschland. Die Kosten- und Einsparungsergebnisse basieren auf durchschnittlichen Kosten- und Zeitschätzungen, die direkt von den Befragten zur Verfügung gestellt wurden. Tatsächliche Kosten und Einsparungen können je nach spezifischem Gerätemix und Bereitstellung variieren. Die ausführliche Studie finden Sie hier.

Leistungsstarke Sicherheit in Windows 11 standardmäßig aktiviert

Surface-Geräte mit Windows 11 enthalten eine Reihe neuer Hardwaresicherheitsfunktionen, die ab Werk aktiviert sind. **Virtualisierungsbasierte Sicherheit (VBS)** und **durch Hypervisor erzwungene Codeintegrität (HVCI)**, auch bekannt als **Speicherintegrität**, dienen dazu, ein noch stärkeres und resilienteres Fundament gegen Angriffe zu schaffen. VBS und HVCI bieten einen besseren Schutz vor gängiger und komplexer Malware und führen im Zusammenspiel sensible Sicherheitsoperationen in einer isolierten Umgebung durch. Indem VBS und HVCI Code noch vor dessen Ausführung überprüft, wird verhindert, dass Malware in den Systemspeicher gelangt. Erlangt eine Bedrohung Zugriff auf Systemressourcen, kann HVCI die Auswirkungen der Malware begrenzen und eindämmen.

Wir liefern Surface-Geräte mit Windows 11 ab Werk mit **aktivierten Sicherheitsfunktionen** aus. Das hilft Sicherheitsverantwortlichen und Führungskräften, sicherheitsorientierte Verhaltensweisen in ihrem Unternehmen zu etablieren und den Wunsch nach Eigenverantwortung in den Teams zu befriedigen.

Noch bevor man sich mit einer der zahlreichen biometrischen Optionen ohne Passwort- oder PIN-Eingabe anmeldet, garantiert **Secure Boot**, dass die Firmware im Werkzustand ist. Zusammen verhindern Secure Boot und Trusted Boot, dass Malware und beschädigte Komponenten während des Starts geladen werden.

Nach dem Start sorgt **BitLocker** dafür, dass Daten selbst auf verlorenen, gestohlenen oder vorschriftswidrig ausgemusterten Geräten unzugänglich sind.

Robuste Cybersicherheit bedeutet nicht mehr nur die Aufrechterhaltung des Schutzes, sondern Resilienz gegenüber aktuellen und zukünftigen Bedrohungen. Cyberresilienz ist eine organisatorische Aufgabe, die von jeder und jedem Einzelnen Eigenverantwortung verlangt. Unternehmen müssen einen integrierten Ansatz verfolgen – mit Sicherheit auf allen Ebenen, vom Chip bis zur Cloud –, damit Beschäftigte und Daten überall geschützt sind.

Möchten Sie mehr über die von Microsoft entwickelten und in Surface, Windows 11 und Microsoft 365 integrierten cyberresilienten Lösungen erfahren? Dann wenden Sie sich noch heute an unser Vertriebs-Team.

Microsoft Surface

Checkliste für Cyberresilienz

Zu berücksichtigende Fragen bei der Bewertung der Auswirkungen Ihrer Geräte auf die Cyberresilienz

Folgende Fragen und Themen verschaffen Ihnen einen Überblick über den Stand Ihres Geräteportfolios:

- ☐ Welche Priorität räumt die Unternehmensleitung der Sicherheit ein, wenn es um Schwachstellen in unseren Endgeräten geht?
- ☐ Wie hoch ist das Budget, das die Unternehmensleitung in Geräteneuanschaffungen zu investieren gedenkt, um die Sicherheit aufrechtzuerhalten?
- ☐ Was würde eine Sicherheitsverletzung kosten?
- ☐ Kennen Sie alle Endpunkte und deren Schwachstellen? Und zwar in puncto Quantität und Qualität.
- ☐ Dürfen Mitarbeitende ihre eigenen Geräte für Arbeitszwecke mitbringen und nutzen?
- ☐ Auf wie viele Lösungen verlassen Sie sich in Ihrer derzeitigen Sicherheitsinfrastruktur?
- ☐ Verwenden Sie mehrere Gerätetypen und Betriebssysteme? Könnten Sie diese konsolidieren?

Mit Führungspersonen über Sicherheit sprechen

Mit diesen Gesprächseinstiegen können Sie eine Diskussion über Sicherheit anstoßen und letztendlich entscheiden, wie Sie die Cyberresilienz stärken möchten:

- Welche Priorität messen wir der Sicherheit unseres geistigen Eigentums, unserer Daten und unserer Beschäftigten bei?
- Was ist wichtiger und in welchem Maße: Sicherheit oder Employee Experience?
- Sind wir den Anbietern gegenüber Verpflichtungen eingegangen oder gibt es Möglichkeiten zur Konsolidierung?
- Ein Zero Trus-Sicherheitsmodell wird unsere Cyberresilienz verbessern. Wie groß ist die Bereitschaft, diesen Wandel in der Sicherheitsmentalität zu vollziehen?

Cyberresilienz ist Teamarbeit

Damit Unternehmen resilient sind, müssen Technologieverantwortliche die Entscheidungsträger*innen aus allen Bereichen des Unternehmens in die Resilienzplanung einbinden.

Rolle	Relevanz der Geräteauswahl	Weiterführende Infos
Chief Financial Officer	ROI bei Geräteinvestitionen	Bewertung des Business Case von Microsoft und Gesamtbetriebskosten
Chief Sustainability Officer	Einklang mit ESG-Zielen	Microsoft Surface Emissions Estimator
Chief Security Officer	Integration in die Sicherheitsinfrastruktur, Schutz von Daten und geistigem Eigentum	Microsoft Surface und Endpunktsicherheit
Personalchef*in	Unterstützung von Produktivität, Vielseitigkeit, Geräten und Employee Experience	Understanding the Role of Modernized PCs in Hybrid Work Environment Optimization

Weiterführende Informationen

Microsoft Security Insider

Microsoft Secure

Mehr über Zero Trust erfahren

In 5 Schritten zu mehr Cyberresilienz

Geschäftsresilienz – Framework zur Cloud-Einführung | Microsoft Learn

Workshop für Chief Information Security Officer (CISO) – Sicherheitsdokumentation | Microsoft Learn

Sie leiten ein kleines Unternehmen?
So können Surface und mehr Sicherheit Potenzial freisetzen.