Windows 11 Pro

Umfassendes Sicherheits-Playbook für die hybride Arbeitsumwelt

Cybersicherheit steht ganz oben auf der Agenda: 88 % der befragten KMUs halten sich für nicht ausreichend auf den Umgang mit Cyber-Bedrohungen vorbereitet.[1]

Im Folgenden finden Sie einige Möglichkeiten, wie eine sichere, zukunftsfähige IT-Infrastruktur Ihr Unternehmen vor Cyberbedrohungen schützen kann:

Verfolgen Sie einen Zero-Trust-Ansatz

Das Zero-Trust-Sicherheitsmodell reduziert das Risiko, indem Datenpunkte wie Benutzeridentität, Standort und Gerätezustand bei jeder Zugriffsanfrage ausnahmslos überprüft werden. Wenn Sie verifiziert sind, haben Benutzende und Geräte nur begrenzten Zugriff auf die benötigten Ressourcen.

Es gibt drei Zero Trust-Grundsätze:

1

Erstens: Explizit verifizieren. Das bedeutet, dass die Authentifizierung und Autorisierung immer auf der Grundlage aller verfügbaren Datenpunkte erfolgt, einschließlich Benutzeridentität, Standort, Gerätezustand, Dienst oder Arbeitslast, Datenklassifizierung und Anomalien.

2

Zweitens: Nutzen Sie den am wenigsten privilegierten Zugang, der den Benutzerzugriff mit Just-in-time- und Just-enough-Zugriff einschränkt, risikobasierte adaptive Richtlinien und Datenschutz, um sowohl Daten als auch Produktivität zu schützen.

3

Drittens: Gehen Sie von einem Verstoß aus. Gehen Sie davon aus, dass der Verstoß auf eine Weise erfolgt, die den Radius des Bruches und den Zugang zu den Segmenten minimiert. Verifizieren Sie die Ende-zu-Ende-Verschlüsselung und nutzen Sie Analysen, um die Erkennung von Bedrohungen und die Abwehrmaßnahmen zu verbessern.

Um einen Zero-Trust-Ansatz zu implementieren, müssen Unternehmen ihre eigenen Daten verstehen und wissen, wo diese Daten gespeichert sind. Zero-Trust-Sicherheit.

Unternehmen müssen den Grad der Datensensibilität und die potenziellen Risiken kennen, um zu bestimmen, wo Zero-Trust zwingend erforderlich ist. Für cloudbasierte Speicher und Anwendungen wie E-Mail-Dienste und Cloud-Datenspeicher ist die Einrichtung einer Zero-Trust-Umgebung sinnvoll und wichtig, um die Risiken zu minimieren. Ohne diesen Ansatz sind die Kennwörter, Geräte und sensiblen Daten des Unternehmens unweigerlich dem Risiko von Angriffen ausgesetzt.

Erweiterte Authentifizierungsmethoden implementieren

Eine Sicherheitsverletzung wird sehr viel wahrscheinlicher, wenn die Methoden zur Benutzerauthentifizierung kompromittiert werden. Ein nicht autorisierter Zugriff auf das Gerät eines Mitarbeitenden verschafft potenziellen Eindringlingen nicht selten Zugriff auf das gesamte Netzwerk eines Unternehmens. In der hybriden Arbeitsumgebung von heute ist es unabdingbar, eine sichere Methode zu implementieren, um sicherzustellen, dass die Benutzenden auch wirklich die sind, für die sie sich ausgeben. Die Multifaktor-Authentifizierung kann viel dazu beitragen, eine sicherere Umgebung zu schaffen. Kennwörter reichen nicht mehr aus, um die immer raffinierteren Bedrohungen abzuwehren, da sie meist leicht kompromittiert werden können. Techniken wie die Zwei-Faktor-Authentifizierung in Kombination mit den biometrischen Funktionen, die auf vielen modernen Geräten verfügbar sind, wie z. B. Windows Hello for Business, sind viel effektiver beim Schutz von Unternehmen und ihren Netzwerken vor Cyberangriffen, insbesondere wenn sie mit einer Zero-Trust-Sicherheitsstrategie verstärkt werden.

Stärkung der Hardware-Sicherheit

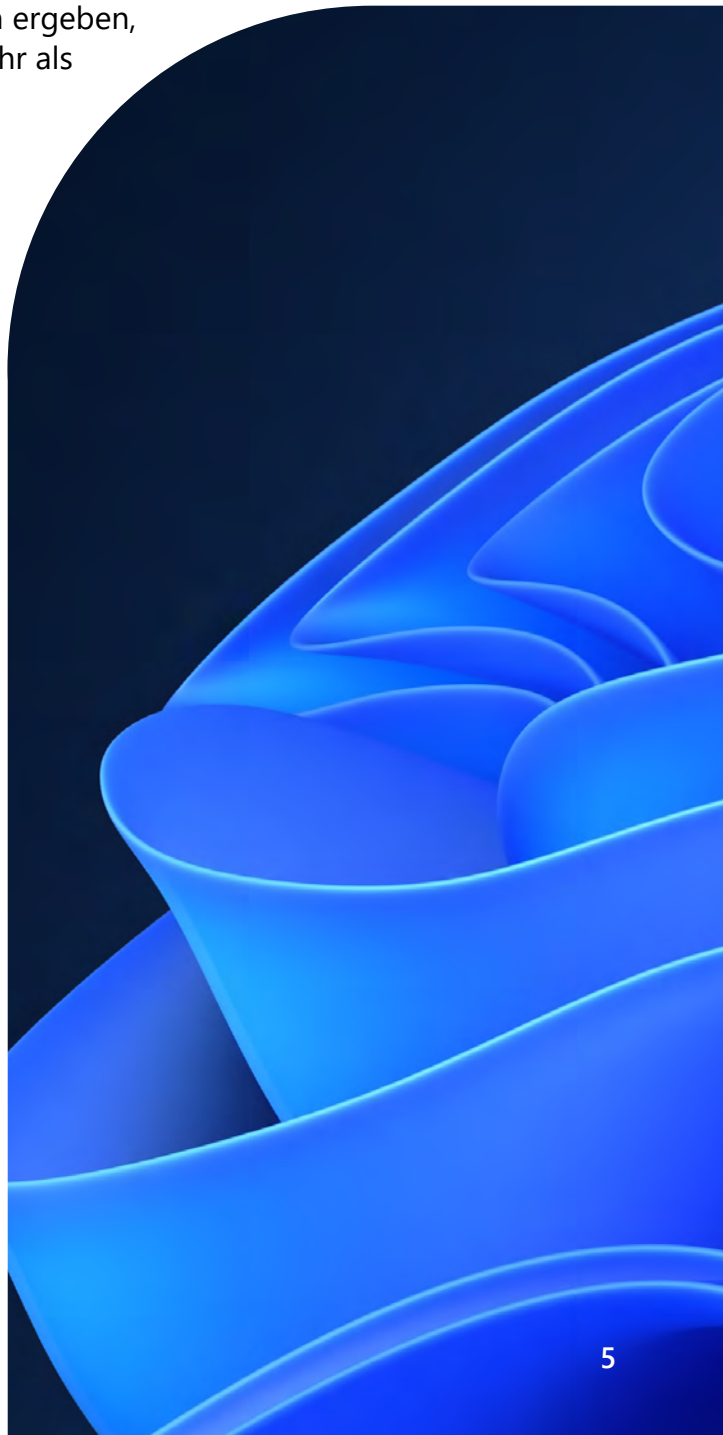
Das Betriebssystem allein bietet keinen zuverlässigen Schutz vor der Vielzahl von Tools und Techniken, die Cyberkriminelle einsetzen können, um einen Computer zu kompromittieren. Eindringlinge können, wenn sie erst einmal drin sind, schwer zu entfernende Schadsoftware in die Firmware des Geräts einschleusen oder sensible Daten und wichtige Anmeldeinformationen stehlen. Es kann schwierig sein, diese Eindringlinge zu entdecken, wenn sie sich erst einmal Zugang verschafft haben. Es muss eine enge Verbindung zwischen Hardware-Sicherheit und softwarebasierten Sicherheitsanwendungen bestehen. Moderne Bedrohungen erfordern Computerhardware, die auf Chip- und Prozessorebene sicher ist und sensible Geschäftsinformationen genau dort schützt, wo sie gespeichert sind. Es gibt ganze Klassen von Sicherheitsrisiken, die einfach durch eingebaute Sicherheitsfunktionen auf der Hardware-Ebene beseitigt werden können.

Solche Funktionen finden Sie zum Beispiel in allen Windows 11 Secured-Core PCs. Darüber hinaus lassen sich erhebliche Leistungsverbesserungen erzielen, wenn man sie mit der Bereitstellung ähnlicher Sicherheitsfunktionen mit Software allein vergleicht. Dies erhöht die allgemeine Sicherheit eines Systems, ohne die Systemleistung zu beeinträchtigen.

Zugriffskontrolle für identitätsbasierten Schutz verwenden

In der Cloud können Administrator*innen Identitäten und Zugriff von einem Ort aus kontrollieren und verwalten. Mit Microsoft Azure Active Directory (Azure AD) können sie zum Beispiel die Identitäten ihrer Mitarbeitenden zentral verwalten sowie Richtlinien für den Zugriff auf Anwendungen, Websites und Gruppen konfigurieren und einsetzen. Administrator*innen können Compliance-Anforderungen einbetten und neue Regeln einfügen, sobald sie entstehen.

Cloud-basierte Steuerungen erhöhen die Sicherheit und stärken die Compliance. Untersuchungen von Microsoft haben ergeben, dass allein durch die Multifaktor-Authentifizierung mehr als 99,9 % der Angriffe zur Kompromittierung von Konten abgewehrt werden können.[2] Der bedingte Zugriff ermöglicht es Administrator*innen, Regeln auf der Grundlage von Aktivitäten oder Standorten zu erstellen, wodurch die Möglichkeiten für Angreifende, Sicherheitsrisiken auszunutzen, weiter eingeschränkt werden. So können beispielsweise Anmeldeversuche, die von außerhalb des Landes oder zu ungewöhnlichen Zeiten erfolgen, abgewiesen werden. Darüber hinaus können Administrator*innen Single Sign-On aktivieren, so dass Benutzende überall sicheren Zugriff auf Anwendungen haben und die Kennwortverwaltung für die IT-Abteilung vereinfacht wird.



Microsoft hat jüngst die allgemeine Verfügbarkeit der Unterstützung für Multi-Cloud-Sicherheit eingeführt. Nun können Unternehmen Multicloud-Ressourcen wie Google Cloud Platform (GCP) und Amazon Web Services (AWS) in das Azure Security Center einbinden und Server mit Azure Defender for Servers auf Basis von Azure Arc schützen.

Remotegeräte schützen

Die Microsoft-Cloud vereinfacht die Verwaltung von Geräten und Anwendungen. Mit Microsoft Intune beispielsweise kann die Gerätebereitstellung sicher und remote verwaltet werden. Außerdem lassen sich Anwendungen problemlos skalieren, um dem Bedarf gerecht zu werden.

Microsoft Windows Autopilot nutzt Sicherheitseinstellungen und andere Steuerungen, um Geräte zu schützen, bevor Mitarbeitende eine Verbindung zu einer Ressource herstellen.

Anwendungen sichern

Erhalten Sie noch mehr Schutz vor nicht vertrauenswürdigen Quellen, indem Sie Dateien und Websites in einem isolierten Container mit Windows Defender Application Guard öffnen. Das Cloud-first Design ermöglicht eine einfache Erweiterbarkeit mit Microsoft 365, Microsoft Defender for Cloud und Microsoft Defender for Endpoints.[3]

Optimieren Sie die Steuerung der Sicherheit an verschiedenen Orten und weiten Sie die Sicherheit auf die Cloud aus. Schützen Sie Geräte, Daten, Apps und Identitäten an jedem Ort. Vertrauen Sie bei der Bereitstellung darauf, dass 99,6 % der Anwendungen mit Windows 11 kompatibel sind.[4]

Sicherheitsmaßnahmen automatisieren

Cloudbasierte Technologien ermöglichen es IT-Administrator*innen, Updates, Patches und Backups automatisch auf alle Systeme und Geräte anzuwenden. Dadurch werden Konfigurationsfehler reduziert und Ausfallzeiten begrenzt. Zudem sind die Systeme zugleich vor neuen Bedrohungen geschützt. Routineaufgaben können automatisiert werden, so dass die Administrator*innen Zeit haben, sich auf wichtige Aufgaben zu konzentrieren, die wirklich ihr Fachwissen erfordern.

Schützen Sie Ihr Unternehmen mit Windows 11 Pro Geräten

Die Verbesserung der Sicherheitslage Ihres Unternehmens sollte Vorrang haben. Die Ausstattung Ihrer Mitarbeitenden mit sicheren Geräten ist der Grundstein für den Erfolg. Die neuen Windows 11 Pro Geräte in Kombination mit Microsoft 365 sind für sicheres hybrides Arbeiten konzipiert.

- Schützen Sie Ihre Mitarbeitenden vor Schadsoftware, Viren, Phishing-Versuchen und bösartigen Links und tragen Sie dazu bei, geschäftskritische Daten zu schützen.

- Profitieren Sie von leistungsstarken Sicherheitsebenen für Geräte, Daten, Identitäten, Anwendungen und die Cloud.

- Optimieren Sie die IT mit einheitlichen, cloudbasierten Endpunkt-Verwaltungstools wie Microsoft Endpoint Manager, Azure Active Directory und Windows Autopilot. Legen Sie Richtlinien fest und setzen Sie sie durch, verwalten Sie Anwendungen und Identitäten und stellen Sie einfach business-ready Geräte bereit – alles remote.

- Überwinden Sie die Hürden der Remote-Zusammenarbeit mit einer einzigen Lösung, die Videokonferenzen, Produktivitätsanwendungen, Dateifreigabe und mehr umfasst. Sorgen Sie dafür, dass Ihre Mitarbeitenden mit einer einheitlichen Lösung für die Zusammenarbeit sicheren Zugriff auf wichtige Arbeits-Apps und Informationen haben.

- Menschen in datenschutzsensiblen Branchen oder Geschäftsszenarien sind Secured-Core PCs die sichersten Windows-Geräte und verfügen über alle erweiterten Sicherheitsfunktionen von Windows 11.

Verringern Sie das Risiko von Cyberangriffen spürbar, indem Sie veraltete PCs durch neue, moderne Geräte ersetzen, die für Sicherheit und hybrides Arbeiten optimiert sind. Windows 11 Pro und Microsoft M365 vereinen Hardware und Software für einen leistungsstarken, sofort einsatzbereiten Schutz für Ihre Geräte, Daten, Anwendungen, Identitäten und Dienste.

Windows 11 Pro

[1] *https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity*

[2] *https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/*

[3] *Separat erhältlich*

[4] *App Assure-Programmdaten von Okt 2018 bis Feb 2022. Seit 2018 hat App Assure mit Tausenden von Kund*innen zusammengearbeitet und über 1,1 Millionen Apps mit einer Kompatibilitätsrate von 99,6 Prozent bewertet. Weitere Informationen finden Sie auf der Website von App Assure und im Windows IT Pro Blog-Beitrag über App Assure*