Microsoft

Schützen Sie Ihre Daten: Sieben Möglichkeiten, Ihre Sicherheitslage zu verbessern

Es steht außer Frage, dass Enterprise Mobility, die unzähligen Geräte am Arbeitsplatz, SaaS-Apps und die Cloud das Geschäftsleben stark verändert haben.

Unternehmen setzen auf Zusammenarbeit und Mobilität, um die Flexibilität zu erhöhen, die Leistung zu steigern und Entscheidungsprozesse zu unterstützen. Insbesondere mobile Geräte und Anwendungen sind leistungsstarke Tools, um ständig produktiv zu sein. Mit der wachsenden Anzahl von mobilen Geräten wird das App-Hosting von eigenen zu öffentlichen oder Netzwerken außerhalb der Domäne verschoben. Etablierte Unternehmensgrenzen lösen sich auf, und für Unternehmen nehmen die Risiken bei Sicherheit und Compliance zu.

Beispielsweise erhöhen mehrfache Anmeldungen, das Speichern von Informationen an unterschiedlichen, nicht verwalteten Speicherorten und der Austausch von Daten ohne umfassenden Schutz die Anfälligkeit für Sicherheitsbedrohungen und das Risiko von Datenverlusten – zum Beispiel die Gefahr, dass Mitbewerber proprietäre Daten stehlen oder wichtige Daten manipuliert oder beschädigt werden. Dies wirft die Frage auf:

Ist es möglich, Ihren Mitarbeitern die gewünschte Mobilität und Produktivität zu gewähren und gleichzeitig Ihre Daten zu schützen?

Ist es möglich, Fachabteilungen die neuen Anwendungen und Systeme nutzen zu lassen, um flexibler zu sein?

In diesem E-Book besprechen wir sieben häufige Bedenken in Bezug auf den Datenschutz für Unternehmern wie Ihres und die Schritte, mit denen Sie die Bedrohungen verringern können. Dies ist das erste in einer Reihe von E-Books, die Microsoft zum Thema Sicherheit veröffentlichen wird.

Sieben Möglichkeiten, Ihre Sicherheitslage zu verbessern

- Bedrohungen im Bereich Identitäts- und Zugriffsverwaltung verringern
- Mobile Geräte und Apps verwalten
- Bedingten Zugriff nutzen
- Schutz von Unternehmensdaten verbessern
- Datenverluste verhindern
- Sichere Zusammenarbeit ermöglichen
- Schadcode abfangen

Bedrohungen im Bereich Identitäts- und Zugriffsverwaltung verringern

Wie Sie wissen, ist es eine erhebliche Herausforderung, die Kontrolle über Anwendungen, die sich über Rechenzentren des Unternehmens und über öffentlichen Cloud-Plattformen erstrecken, zu behalten. Mitarbeiter möchten von verschiedenen Standorten und Geräten aus auf Datenressourcen zugreifen. Und im Netzwerk benötigen sie Zugriff auf verschiedene Ressourcen, die sich stetig ändern. Zudem fordern Mitarbeiter unter Umständen den Zugriff auf Unternehmensressourcen an, die sie für ihre Arbeit benötigen, wenn sie nicht im Büro sind.

Leider sind Mitarbeiter häufig das schwächste Glied, entweder durch das versehentliche Offenlegen vertraulicher Daten oder das Preisgeben ihrer Anmeldeinformationen in sozialen Netzwerken. Ein externer Angreifer könnte diese Anmeldeinformationen nutzen, um auf das Netzwerk zuzugreifen und Kundendaten, geistiges Eigentum und andere sensible Daten zu stehlen. Auch interne Sicherheitsverstöße können Ihre Daten Risiken aussetzen. Wie stellen Sie die Kontrolle über die Art, die Zeit, den Ort und die Personen eines Anwendungszugriffs sicher?

Identitäts- und Zugriffsverwaltung kann das Risiko verringern.

- Eine einzige Identität ersetzt mehrere Anmeldeinformationen für den Zugriff auf lokale und Cloud-Ressourcen.
- Beschränken Sie den Zugriff einzelner Benutzer darauf, was Mitarbeiter brauchen, um ihre Aufgaben zu erledigen.
- Entziehen Sie Zugriffsrechte, wenn sich die Rollen eines Mitarbeiters ändern, er das Unternehmen verlässt oder keinen Zugriff mehr auf bestimmte freigegebene Ressourcen benötigt.
- Erzwingen Sie die zweistufige Authentifizierung basierend auf riskantem Verhalten.

- *Über 80 Prozent aller Mitarbeiter nutzen bei ihrer täglichen Arbeit nicht genehmigte SaaS-Anwendungen.*[1]

[1] Quelle: „Die Schatten-IT: Sechs Trends mit Auswirkungen auf die Sicherheit." (Frost & Sullivan)

Weitere Informationen:

- *Identitäts- und Zugriffsverwaltung*

Mobile Geräte und Apps verwalten

Durch die Zunahme des Bring Your Own Device (BYOD)-Trends und die Nutzung von Software-as-a-Service (SaaS)-Anwendungen vervielfachen sich die Sicherheitsbedenken. Wenn Unternehmen stärker auf SaaS-Anwendungen setzen, werden kritische Daten in der Public Cloud gespeichert, unterliegen daher größeren Risiken und unterliegen nicht denselben Standards wie die heutige IT.

Jedes Mal, wenn Geräte gestohlen werden, verloren gehen oder nur unbeaufsichtigt bleiben, sind Ihre Daten Angriffen ausgesetzt und unzureichend geschützt. Sie sind auch Angriffen ausgesetzt, wenn Ihre Unternehmensdaten in private Anwendungen gelangen und so in die falschen Hände geraten können. Wie können Sie in den Zeiten von BYOD Ihre Daten schützen, ohne die Mitarbeiterproduktivität zu beeinträchtigen?

Beginnen Sie mit den Grundlagen:

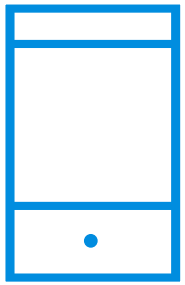
- Unterbrechen Sie den Benutzerfluss nicht, machen Sie die Compliance für sie einfach und natürlich
- Machen Sie transparent, was die IT auf ihren Geräten ausführt
- Schützen Sie nur die Unternehmensdaten

- *Ungefähr 52 Prozent der Informationsarbeiter in 17 Ländern geben an, dass sie bei der Arbeit mehr als drei Geräte nutzen.*[1]

[1] Quelle: „Employee devices bring added security concerns" von Cindy Bates (Microsoft US Small and Midsize Business Blog)

Weitere Informationen:

- *Microsoft Intune*



Bedingten Zugriff nutzen

Bedingter Zugriff beschränkt den Zugriff auf Unternehmensressourcen basierend auf Benutzeridentität oder Geräteintegrität. Dabei geht es auch um das Erzwingen von Richtlinien basierend auf Standort und Vertraulichkeit der Anwendungsdaten.

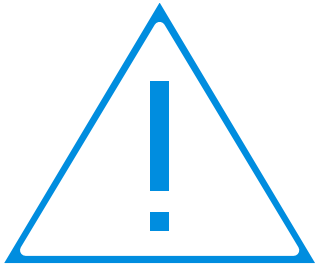
Beispielsweise erfordert der Zugriff auf eine Customer Relationship Management (CRM)-Anwendung aus einem Café eine mehrstufige Authentifizierung wegen des Standorts des Benutzers und der sensiblen Daten des CRM-Systems. Ein anderes Beispiel wären E-Mails. Ein Gerät muss zum Zugriff auf geschäftliche E-Mails Richtlinien wie Verschlüsselung und PIN erfüllen.

Was sind Ihre ersten Schritte?

- Etablieren Sie Zugriffsrichtlinien für mobile Geräte. Sie können entweder die vollständige Verwaltung des Geräts oder nur der Anwendungen wie Outlook für den Zugriff auf geschäftliche E-Mails zur Voraussetzung machen.
- Nutzen Sie dynamische Gruppen, um Mitarbeitern den Zugriff auf die Anwendungen zu ermöglichen, die sie je nach ihren Rollen benötigen.
- Erzwingen Sie eine Multi-Faktor-Authentifizierung, dadurch wird eine zusätzliche Datenschutzebene geschaffen, weil Benutzer sich auf zwei Arten authentifizieren müssen. Die erste Methode kann die herkömmliche Kombination aus Benutzernamen und Kennwort sein. Die zweite Methode beinhaltet häufig eine physische Komponente, deren Duplizierung praktisch unmöglich ist. Beispielsweise das Durchziehen einer Schlüsselkarte und Eingeben einer PIN, Anmelden bei einer Website und Verwenden eines einmaligen Kennworts, Anmelden über einen VPN-Client mit einem digitalen Zertifikat oder das Scannen des Fingerabdrucks eines Benutzers.

Weitere Informationen:

- *Bedingter Zugriff mit Azure Active Directory*
- *Übersicht über bedingten Zugriff*
- *Bedingter Zugriff mit Microsoft Intune*
- *Office 365 mit Microsoft Intune*
- *Windows 10*



Schutz von Unternehmensdaten verbessern

Wenn Sie Mitarbeitern die Nutzung ihrer eigenen Geräte gestatten, erhöht dies das Risiko für das versehentliches Offenlegen von Daten durch Apps und Dienste wie E-Mail, soziale Medien und die Cloud. Diese befinden sich außerhalb Ihrer Kontrolle. Beispielsweise kann ein Mitarbeiter aktuelle Bilder aus der Entwicklung über sein privates E-Mail-Konto versenden, Informationen in Beiträge in sozialen Medien kopieren oder einen Bericht in Bearbeitung in seinem persönlichen Cloud-Speicher ablegen. Sie möchten persönliche Geräte zulassen, ohne jedoch die Sicherheit Ihrer Daten zu beeinträchtigen. Wie können Sie beides erreichen?

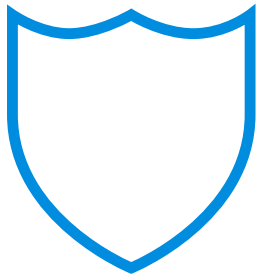
Der Unternehmensdatenschutz (Enterprise Data Protection, EDP) kann vor diesen möglichen Offenlegungen von Daten über nicht autorisierte Apps oder Standorte schützen, ohne die Nutzererfahrung zu beeinträchtigen.

Erste Schritte:

- Aktivieren Sie EDP in Ihrer Unternehmensumgebung zum Verwalten und Reglementieren von Apps und Daten, ohne nicht notwendige Änderungen vorzunehmen.

Weitere Informationen finden Sie unter:

- *Windows 10 Enterprise Data Protection*
- *BitLocker – Übersicht*
- *Microsoft Intune*



Datenverluste verhindern

Irren ist menschlich, allerdings können die Kosten dafür hoch sein, wie wir alle wissen. Der Austausch von Dokumenten über E-Mails ist ein wichtiges Produktivitätstool für Mitarbeiter, doch daraus ergibt sich für Sicherheitsexperten ein Problem: Wie können Mitarbeiter Dateien per E-Mail austauschen, ohne Ihre vertraulichen Daten zu gefährden?

Beginnen Sie damit, die Wahrscheinlichkeit eines Datenlecks zu reduzieren:

- "Erfahren Sie mehr über die Funktionen zur Verhinderung von Datenverlust (DLP) in Ihrem Ökosystem, um die Daten beim Speichern, Verschieben und Teilen zu schützen. Beispielsweise kann die Verteilung einer E-Mail auf die Organisation begrenzt werden oder sie kann mit einer digitalen Rechteverwaltungsqualifizierung ausgestattet werden, die einschränkt, wer sie öffnen kann.
- Erweitern Sie DLP auch über E-Mails hinaus. Bestimmte Textverarbeitungs-, Tabellen- und Präsentationsprogramme bieten ebenfalls Optionen für den eingeschränkten Zugriff, die verhindern, dass nicht autorisierte Benutzer Dokumente öffnen können.

Weitere Informationen finden Sie unter:

- *Data Loss Prevention (DLP) in Office 365*
- *Microsoft Office 365*

Sichere Zusammenarbeit ermöglichen

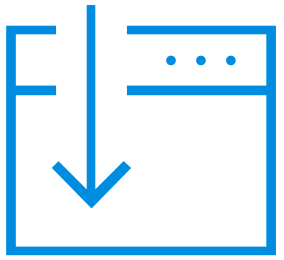
Beim Austausch von Daten geht Bequemlichkeit häufig vor Sicherheit, was für Sicherheitsexperten zu einem wahren Albtraum werden kann. Mitarbeiter können bei ihren Methoden zur Weitergabe von Daten ziemlich kreativ werden, wodurch sie Ihre Daten gefährden und das Unternehmen der Gefahr aussetzen, kritische Daten zu verlieren. Wie fördern Sie die Zusammenarbeit der Mitarbeiter und minimieren gleichzeitig die Risiken durch manipulierte Daten?

Bieten Sie eine flexible, benutzerfreundliche, sichere Lösung an, die ihre Bedürfnisse erfüllt.

- "Stellen Sie sichere Tools für den Austausch von Daten bereit, und stellen Sie sicher, dass die richtigen Mitarbeiter Zugriff haben. Dies umfasst eine sichere Lösung zum Teilen von Dokumenten wie zum Beispiel SharePoint, eine Netzwerkfreigabe mit eingeschränktem Zugriff oder eine cloudbasierte Lösung.
- Machen Sie die Verwendung einer digitalen Rechteverwaltungs- oder einer anderen sicheren E-Mail-Lösung zum Senden sensiblen Materials per E-Mail zur Voraussetzung.
- Stellen Sie einen einfachen und sicheren Workflow für den Austausch von Daten bereit, um die interne und externe Zusammenarbeit zu ermöglichen.

Weitere Informationen::

- *Azure Rights Management*
- *Freigabe geschützter Dateien*
- *Senden verschlüsselter E-Mails*
- *Microsoft Office 365*
- *SharePoint*
- *Microsoft Azure*



Schadcode abfangen

Infektionen durch Schadsoftware gehen häufig auf Benutzerfehler zurück. Phishing- und Spoofing-Anfriffe sind extrem ausgeklügelt geworden. Benutzer erhalten gefälschte E-Mails von vertrauenswürdigen Marken und werden mit gefälschten Meldungen angelockt und überzeugt, scheinbar harmlose Apps herunterzuladen, die versteckte Angriffe enthalten. Sie können nicht verhindern, dass Benutzer im Internet surfen, soziale Medien nutzen oder auf eigenen Geräten auf persönliche E-Mails zugreifen. Wie können Sie ihnen helfen, diese alltäglichen Aufgaben sicherer durchzuführen?

Schulung ist die erste Verteidigungslinie.

- Fordern Sie Ihre Mitarbeiter auf, grundlegende Empfehlungen zu lesen und/oder an Schulungen teilzunehmen, die häufige Methoden von Angriffen durch Schadsoftware erläutern.
- Überprüfen Sie URLs in E-Mails, um sicherzustellen, dass sie relevant, korrekt und legitim sind.
- Empfehlen Sie, dass Mitarbeiter nur aus einer vertrauenswürdigen Quelle heruntergeladene Apps nutzen.

Weitere Informationen:

- *Windows 10*
- *Windows Defender*
- *Windows Device Guard*
- *Microsoft Office 365*

Konzentration auf diese sieben Punkte und Verbesserung der Sicherheit Ihres Unternehmens

Wenn Sie Mitarbeitern die Nutzung mobiler Geräte gestatten, muss dies nicht heißen, dass die Sicherheit Ihrer Daten gefährdet ist. Mit entsprechender Planung, den richtigen Tools und Schulung können Sie Ihren Mitarbeitern die Freiheit einräumen, jederzeit und von überall aus zu arbeiten und gleichzeitig das Risiko zu minimieren.

Weitere Informationen zur Cybersicherheit