How-to-Guide:

So arbeiten Sie sicher und produktiv

Die **Sicherheit von Daten, Anwendungen und Prozessen** sowie die **rechtskonforme Nutzung von IT-Technologien** sind elementare Grundbedürfnisse der digitalen Gesellschaft und wichtige Rahmenbedingungen für Innovationen.

Auch für Unternehmen ist eine sichere IT-Infrastruktur unerlässlich, die ihre Mitarbeiter und Daten vor Angriffen und Diebstahl von außen genauso schützt wie vor Datenpannen und -missbrauch von innen. Doch die Voraussetzungen hierfür sind nicht mehr das, was sie vor ein paar Jahren waren, als einzelne Angreifer die IT von Unternehmen mit Malware und Viren zu kapern versuchten und Firmen nicht im dem Maße vernetzt waren, wie sie es heute sind. Die Abschottung der unternehmenseigenen IT über Firewalls von der Außenwelt reicht für eine umfassende Absicherung nicht mehr aus. In einer mobilen und vernetzten Arbeitswelt müssen Daten und Anwender anders geschützt werden als früher. Statische Sicherungssysteme funktionieren nicht mehr. Die Veränderungen der Bedrohungsszenarien in einer mobilen Welt zu erkennen und eine umfassende Sicherheitsstrategie zu entwickeln, ist eine strategische Unternehmensaufgabe.

In diesem How-to-Guide beschäftigen wir uns mit den naheliegenden, operativen Fragen:
Mit welchen Schritten kann die IT-Abteilung eines Unternehmens schon heute für ein Plus an Sicherheit sorgen?
Wir zeigen Ihnen Tools und Kniffe, die Sie einfach in der Praxis anwenden können.

Schritt 1: Analyse

Nicht alle Daten und Geräte sind für Eindringlinge von außen interessant. Erste Aufgabe der IT-Abteilung ist es daher, sich einen Überblick über Anwendungen, Geräte und Daten zu verschaffen, die es besonders zu schützen gilt, weil sie zum Beispiel mobil von verschiedenen Geräten und Anwendern (Mitarbeiter, Kunden, Partner) genutzt werden. Wichtig sind auch die Schnittstellen zwischen mobilen Geräten und Firmenanwendungen, weil sie potenzielle Einfallstore für Angriffe sind. Wir empfehlen Ihnen dafür Cloud App Discovery, eine Premium-Funktion von Azure Active Directory, die Ihnen bei der Analyse hilft. Nutzen Sie für die Analyse zudem unsere Checkbox.

Angriffspunkte identifizieren

- ☐ Identifizieren Sie, welche Abteilungen sensible Daten intern und nach außen austauschen.
- ☐ Identifizieren Sie, welche Nutzer besonders häufig außerhalb des lokalen Netzwerkes tätig sind.
- ☐ Identifizieren Sie, welche Apps oder Browser-basierte Anwendungen in Ihrem Unternehmen oder direkt von den Fachbereichen verwendet werden. Viele Anwendungen werden ohne das Wissen und den Support der IT-Abteilungen eingesetzt und bilden mitunter eine enorme Sicherheitslücke.

Schritt 2: Konkrete Maßnahmen

Um Unternehmensdaten vor Verlust, Diebstahl und beabsichtigter wie unbeabsichtigter Weitergabe zu schützen, sollten Sie alle Schnittstellen überwachen, über die potentiell Daten verloren gehen oder abgegriffen werden können. Das betrifft zuallererst alle mobilen Geräte, die von außen auf Firmendaten zugreifen können. Darüber hinaus gehören aber auch Webanwendungen, Daten, die für externe Nutzer oder Zwecke bereitgestellt werden, und nicht zuletzt die Zugriffsrechte der Benutzer dazu. Ein einfaches Mobile Device Management (MDM) reicht da nicht mehr aus.

Sie sollten sich daher auf folgende vier Bereiche konzentrieren:

Microsoft

1. Anwender

Mehr Sicherheit bedeutet für Anwender in der Regel mehr Aufwand für den Schutz von (mobilen) Geräten und Daten. **Passwörter** mussten früher regelmäßig erneuert werden, und der Schutz von Daten war eine proaktive Aufgabe, die einen guten Teil der Aufmerksamkeit der Anwender in Anspruch nahm. Der Aufwand der IT-Abteilungen für die **Kontrolle der Benutzerkonten** oder für die **Verwaltung der Accounts**, wenn Zugangsdaten vergessen wurden, war beträchtlich. Indem Sie Berechtigungen – wann immer möglich – Gruppen anstatt einzelnen Anwendern zuweisen, können Sie Zeit sparen und verbessern Ihren Überblick über die vergebenen Rechte.

Maßnahmen für den Anwenderschutz

- Bieten Sie den Mitarbeitern Ihres Unternehmens Single Sign-on an – sowohl für Cloud-Anwendungen als auch Anwendungen, die im eigenen Rechenzentrum laufen. Damit entfällt die Notwendigkeit, sich für jede Anwendung und an jedem Gerät einzeln anmelden zu müssen. Zudem wird die Menge an schwer zu merkenden Passwörter deutlich reduziert.
- Das dafür notwendige Plus an Sicherheit erreichen Sie über Multi-Faktor-Authentifizierungen (MFA), bei denen mehrere Anmeldeverfahren, zum Beispiel ein Passwort und ein Fingerabdruck, Telefonanruf oder eine SMS, in Kombination verwendet werden. Im Rahmen von Windows 10 ist das Anmelden über biometrische Daten möglich. MFA im Rahmen von Microsoft Azure kann auch mit allen anderen Betriebssystemen genutzt werden.
- Definieren Sie in Bezug auf Länge, Komplexität und Änderungsrhythmus praktikable Regeln für Passwörter.
- Setzen Sie auf die Eigenverantwortlichkeit Ihrer Mitarbeiter und ermöglichen Sie ihnen zum Beispiel, Kennwörter selbst zurücksetzen zu können („Self Service“). Der Vorteil: Die Mitarbeiter können schnell selbst aktiv werden, wenn sie ihr Passwort vergessen haben, und müssen nicht auf die IT-Abteilung warten.
- Wirksame Sicherheitsmaßnahmen müssen nicht komplex sein: Teilen Sie Nutzer in Gruppen ein und weisen Sie Rechte, wann immer möglich, diesen Gruppen zu statt einzelnen Anwendern. Solche Gruppen. erleichtern der IT auch das Zuweisen von Richtlinien („Policies“).
- Bieten Sie Ihren Mitarbeitern kompakte Schulungen an, in denen Sie Ihnen die wichtigsten Grundlagen zu IT-Sicherheit und Datenschutz vermitteln und zeigen Sie Ihnen ganz konkret, welche Tools und Routinen Sie in Ihrem Unternehmen einsetzen.

Ergebnis

- ✓ Benutzerfreundlichkeit für die Mitarbeiter
- ✓ Mehr Sicherheit durch Mehrfaktor-Authentifizierung
- ✓ Freie Ressourcen bei der IT durch Gruppenzuweisungen und Self-Service der Mitarbeiter

Microsoft

2. Geräte

Immer mehr Mitarbeiter nutzen **private Geräte** auch beruflich oder berufliche Geräte auch privat. Die Unternehmens-IT sollte beide Arten von mobilen Geräten vor **Diebstahl und Datenverlusten** schützen, die entstehen können, wenn sie berufliche Daten mit privaten Apps öffnen oder speichern. Moderne Lösungen für das Mobile Device Management können diesen Austausch und das Vermischen privater und beruflicher Anwendungen und Daten unterbinden. Bei all diesen Maßnahmen muss die **Privatsphäre** der Mitarbeiter respektiert werden. Auf private Daten und Anwendungen darf das Unternehmen keinen Zugriff haben.

Maßnahmen zur Gerätesicherheit

- Moderne Verwaltungslösungen für mobile Geräte, zum Beispiel die Enterprise Mobility Suite (EMS) von Microsoft, bieten alle Funktionen an, die Sie brauchen, um mobile Geräte mit gängigen Betriebssystemen zu sichern und Daten zu schützen. Über eine Konsole lassen sich neben Windows- auch iOS- und Android-Geräte einbinden und verwalten. Damit entfällt für die IT die Notwendigkeit, für jede Geräteart ein spezielles Tool verwenden zu müssen.

  > Single-Sign-On vereinfacht den Zugang zu Microsoft-Anwendungen sowie zu mehr als 2.500 Applikationen anderer Anbieter, darunter Dropbox, Salesforce oder Google Apps. Anwendern reicht ein Passwort für die Anwendung, die damit über dieselbe Sicherheit verfügen, wie die Applikationen von Microsoft. Im zweiten Schritt bringt die Mehrfaktor-Authentifizierung zusätzliche Sicherheit.

  > Sollte es zu einem Verlust oder Diebstahl eines Gerätes kommen, ist es notwendig, dass Sie als IT über Fernzugriff auf das Gerät zugreifen können und sensible Daten löschen können.

- All diese Funktionen lassen sich über Policies weitgehend automatisieren und an die angeschlossenen Geräte ausspielen. Das sorgt für Sicherheit und reduziert den administrativen Aufwand.

- Prüfen Sie, ob Sie Ihre Unternehmensanwendungen und -daten über ein firmeneigenes Web-Portal für den mobilen Zugriff zur Verfügung stellen können. Ein solches Firmenportal erleichtert der IT die Rechtezuweisung für Apps, etwa um zu verhindern, dass sensible Firmendaten auf privaten Geräten gespeichert werden können.

Ergebnis

- ✓ Die Geräte im mobilen Einsatz sind einfach sicher zu bedienen und vor Diebstahl und Datenverlust geschützt.
- ✓ Mit Management-Tools wie EMS hält sich der Administrationsaufwand für mobile Geräte wie Smartphones, Tablets oder Notebooks in Grenzen.
- ✓ Über firmeneigene Web-Portale ermöglichen Sie Nutzern, sich Anwendungen selbstständig runterzuladen, die durch die IT bereits verwaltet werden. Der Spielraum für „Schatten-IT“ wird damit verringert.

Microsoft

3. Anwendungen

Um die Anwendungslandschaft Ihres Unternehmens optimal schützen zu können, braucht Ihre IT-Abteilung zunächst einmal einen Überblick darüber. Unterschätzen Sie dabei nicht die so genannte Schatten-IT: Anwendungen, die von Fachbereichen oder einzelnen Mitarbeitern erworben wurden und eingesetzt werden. Finden Sie heraus, über welche Applikationen die Anwender Daten bearbeiten: Sind es nur lokale oder auch Web-Anwendungen?

Sind es firmeneigene Anwendungen in den Fachabteilungen (Line-of-Business-Apps) oder Software-as-a-Service-Applikationen (SaaS) wie Office 365 oder Google Apps aus der Cloud?

Maßnahmen zum Schutz von Anwendungen

- Über ein firmeneigenes Web-Portal können Sie den Anwendern die Installation nützlicher Programme via Self-Service durch die Mitarbeiter erleichtern: Ihre Mitarbeiter können sich selbstständig die Anwendungen runterladen, die sie benötigen. Diese Anwendungen sind bereits durch die IT vorkonfiguriert und erfüllen somit alle notwendigen Sicherheitsanforderungen.
- Stellen Sie sicher, dass Unternehmensdaten nicht in einer Unternehmensanwendung (zum Beispiel Outlook) geöffnet und dann in einer privat genutzten App (wie Facebook) geteilt, bearbeitet oder gespeichert werden können. Das kann die IT über Mobile Application Management (MAM) sicherstellen.
- Prüfen Sie den Einsatz einer kompletten Verwaltungslösung für alle mobilen Szenarien inklusive MDM und MAM. All das kann die Enterprise Mobility Suite (EMS).
  Hier können Sie unterschiedliche Gerätetypen, Betriebssysteme, Plattformen und Anwendungsarten (wie firmeneigene und SaaS-Applikationen) von einer einzigen Konsole aus verwalten.

Ergebnis

- ✓ Die Reduktion auf eine Verwaltungskonsole spart Zeit in der IT-Verwaltung.
- ✓ Self-Service für die Mitarbeiter minimiert die Helpdesk-Anfragen bei der IT, gibt den Anwendern größere Reaktionsmöglichkeiten und dämmt zusätzlich die Verwendung nicht zertifizierter Anwendungen ein.
- ✓ Die unterschiedliche Regelung des Umgangs mit Firmendaten in beruflich und privat genutzten Anwendungen sorgt für mehr Datensicherheit im Unternehmen.

Microsoft

4. Dokumente

Das in Dokumenten gespeicherte Wissen ist das wertvollste Gut von Unternehmen. Es gehört daher zu den wichtigsten Aufgaben der IT, die Sicherheit von Dokumenten zu gewährleisten – auch dann, wenn sie mit Dienstleistern oder anderen externen Stellen ausgetauscht werden. Das gilt insbesondere, wenn die Daten das lokale Netzwerk verlassen und zum Beispiel über öffentliches WLAN versendet werden. Es sollte sichergestellt werden, dass nur die Anwender auf ein Dokument zugreifen können, die die dafür nötigen Rechte zugewiesen bekommen haben. Über solche automatischen Schutzmechanismen hinaus müssen die Mitarbeiter auch wissen, welche Informationen sie versenden dürfen, und welche nicht. Zu den schutzwürdigen Informationen zählen zum Beispiel alle personenbezogenen Daten eines Unternehmens über Mitarbeiter und Kunden. Da nicht jeder Mitarbeiter immer einschätzen kann, wann ein Dokument schützenswert ist und wann nicht, sollten ihm hier Hilfestellungen durch die IT sowie die Rechtsabteilung angeboten werden.

Maßnahmen zur Dokumentensicherheit

- Die IT kann je nach Abteilung und nach Begrifflichkeiten im Dokument vorgeben, wann ein Dokument schützenswert ist.
- Ist z.B. Azure Rights Management (Azure RMS) aktiviert, kann jeder Mitarbeiter individuell Daten geschützt nach außen versenden. Dabei kann er selbst Empfänger und Bearbeitungszeitraum sowie bestimmte Berechtigungen wie „Inhalt anzeigen", „Datei speichern", „Weiterleiten" oder „Antworten" festlegen.
- Für viele Organisationen sind diese Standardvorlagen bereits ausreichend. Die IT kann aber auch eigene, benutzerdefinierte Vorlagen für Rechterichtlinien erstellen. Das ist zum Beispiel dann sinnvoll, wenn Sie innerhalb von Gruppen oder innerhalb von Dokumenten unterschiedliche Rechte vergeben möchten (zum Beispiel „Anzeigen" und „Bearbeiten" erlauben, „Kopieren" und „Drucken" aber untersagen).
- Über die so genannte Compliancesuche im Office 365 Compliance Center haben Sie als IT-Administrator die Möglichkeit, Postfächer, SharePoint Online-Websites sowie OneDrive for Business-Speicherorte in Ihrer Office 365-Organisation nach vertraulichen und personenbezogenen Daten zu durchsuchen. Damit können sie den Abfluss interner und vertraulicher Daten aus dem Unternehmen kontrollieren und ggf. unterbinden.

Ergebnis

- ✓ Diese Maßnahmen stellen sicher, dass sich das Unternehmen mit seinen Mitarbeitern und Daten Compliancegerecht verhält.
- ✓ Sie geben auch den Mitarbeitern die Sicherheit, die sie für den alltäglichen Umgang mit sensiblen und vertraulichen Informationen benötigen.

Microsoft

14 Sicherheitstipps für Anwender

Mit den folgenden vierzehn Verhaltensregeln können auch die Anwender selbst für bestmögliche Sicherheit von Geräten und Daten sorgen. Bei einigen Regeln sollten Sie allerdings die Hilfe Ihrer IT-Abteilung in Anspruch nehmen.

1 Schützen Sie mobil genutzte Geräte, Anwendungen und Daten über eine mehrstufige Authentifizierung (MFA=Multi-Faktor-Authentifizierung) der Nutzer vor fremdem Zugriff. Dafür brauchen Sie ein Passwort, das sie aber auf einem zweiten Weg bestätigen. Dies kann entweder durch einen Anruf, eine SMS oder eine PIN geschehen.

2 Richten Sie zusätzlich – falls vorhanden – Funktionen zum Wiederfinden Ihres Geräts bei Verlust ein (bei Windows Phone zum Beispiel finden Sie in den Einstellungen unter Datenschutz die Funktion Mein Handy finden.)

3 Sperren Sie immer den Bildschirm Ihrer Geräte, auch Ihres Desktop-PCs am Arbeitsplatz und Ihres Mobiltelefons. Nutzen Sie die Sperre selbst dann, wenn Sie ihr Gerät nur kurz unbeaufsichtigt lassen.

4 Schützen Sie vertrauliche Dokumente stets mit einem Passwort. Sie finden diese Einstellung beispielsweise in Word und Excel im Überprüfen-Menu unter Dokument schützen bzw. Blatt oder Arbeitsmappe schützen oder im Menü Speichern unter (hängt von der verwendeten Version ab). Teilen Sie diese Dokumente und das dazugehörige Passwort nicht in derselben Mail oder Chatnachricht.

5 Lassen Sie keine gedruckten Dokumente mit vertraulichen Informationen offen liegen.

6 Sichern Sie vor allem externe Laufwerke und USB-Sticks vor Diebstahl. Dafür eignet sich die BitLocker-Laufwerkverschlüsselung, die Teil von Windows ist. Damit verhindern Sie, dass jemand ohne die dafür notwendige Berechtigung auf Daten Ihrer Speichermedien zugreifen kann. Schützen Sie auch die internen Laufwerke Ihrer Rechner über BitLocker. So verhindern Sie auch den Zugriff auf Systemdateien, die Hacker zum Ausforschen von Passwörtern benötigen.

7 Schreiben Sie Ihre Passwörter niemals auf und speichern Sie sie nicht! Nutzen Sie Passwortregeln dafür, wie sie zum Beispiel hier nachzulesen sind. Mit dem Microsoft-Passwortprüfer können sie die Stärke Ihres Kennworts prüfen.

8 Senden Sie niemals sensible Daten an Ihre private Mailadresse und speichern Sie keine Firmendokumente auf privaten Geräten oder privaten Speicherorten.

9 Versenden Sie Dokumente an externe Partner sowie im öffentlichen WLAN nur mit Dokumentenschutz. Dafür bieten die Rights Management Services (RMS) beispielsweise von Windows oder Azure auch die Möglichkeit, einem Dokument eine bestimmte E-Mail-Adresse zuzuordnen. Andere Empfänger, als der bestimmte, können dieses Dokument dann nicht öffnen. Sprechen Sie dazu mit Ihrer IT-Abteilung.

10 Geben Sie Ihre mobilen Geräte (auch die privaten, die Ihre Mitarbeiter beruflich nutzen) zur Verwaltung in die IT, um wichtige Richtlinien und Anwendungen installieren und den Zugriff durch andere Nutzer beschränken zu lassen.

11 Sprechen Sie die Verwendung von (neuen) Online- und spezifischen Abteilungsanwendungen mit der IT ab, damit diese einen sicheren Datenaustausch gewährleisten kann.

12 Wenn Mitarbeiter in andere Abteilungen wechseln oder das Unternehmen verlassen, lösen Sie deren spezifische Zugriffsrechte auf, etwa auf Finanztools oder Kundendatenbanken.

13 Führen Sie in Kooperation mit der IT-Abteilung Ihres Unternehmens regelmäßig Software-Updates durch, um immer die aktuellste und vor allem sicherste Software einsetzen zu können.

14 Die beste Vorsorge gegen den Verlust wertvoller Firmendaten ist eine Backup-Strategie für Ihre Daten – egal, ob sie in der Cloud lagern, oder in im firmeneigenen Rechenzentrum. Wir empfehlen Ihnen dafür zum Beispiel Azure Backup aus der Cloud.

Zum Vertiefen

- Das Microsoft-Kompendium IT-Compliance und -Security bietet IT-Abteilungen und Anwendern Hilfestellungen für den Aufbau eines unternehmensweiten Sicherheitssystems, Hintergrundwissen zu aktuellen Themen, innovativen Produkten und Technologien sowie Handlungsempfehlungen und Informationen rund um die Themen IT-Compliance & IT-Governance.
- Auf der PinPoint-Website finden Sie bei Bedarf Microsoft-Partnerunternehmen, die Sie bei Sicherheitskonzepten und Lösungen kompetent beraten.
- Hier finden Sie eine Übersicht über die Enterprise Mobility-Lösungen von Microsoft.
- In seinen Trust Centern gibt Microsoft ausführlich Auskunft über seine Werkzeuge und Mechanismen, mit denen das Unternehmen den Schutz der Kundendaten sicherstellt:
  - Office 365 Trust Center
  - Microsoft Azure Trust Center
  - Microsoft Dynamics CRM Trust Center
  - Microsoft Intune Trust Center
- Im Microsoft Safety & Security Center finden Sie (auf Englisch) eine umfassende Übersicht über die Sicherheits-Tools und Funktionen der Microsoft-Plattformen und Produkte sowie zahlreiche Tipps für die praktische Annäherung an den Daten- und Geräteschutz im Unternehmen.