Microsoft

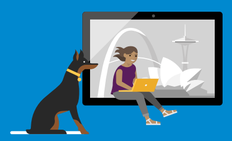
Gehen Sie auf Nummer sicher

Schützen Sie die Daten Ihres Unternehmens mit vertrauenswürdiger Microsoft-Software.

Herausragende Sicherheit für Ihr Unternehmen

Windows 10 ist das sicherste Windows, das Microsoft je entwickelt hat: mit mehrschichtigem Ansatz zum Schutz Ihres Unternehmens vor aktuellen Sicherheitsbedrohungen. Mit den Sicherheitsfeatures von Windows 10 müssen Sie sich keine Sorgen darum machen, dass Mitarbeiter versehentlich Informationen preisgeben: dank verschlüsselter Daten und Gerätesperrung bei Verlust oder Diebstahl. Durch diesen umfassenden Ansatz wird der Ruf Ihres Unternehmens optimal geschützt.

Sicherheitsfeatures von Windows 10



Geräteschutz

UEFI Secure Boot

Windows Trusted Boot

Identitätsschutz

Windows Hello**

Credential Guard

Information Protection

Windows Information Protection

BitLocker und BitLocker To Go***

Angriffserkennung, -untersuchung und -abwehr

Windows Defender Advanced Threat Protection

Bedingter Zugriff

Bedrohungsabwehr

Microsoft Edge

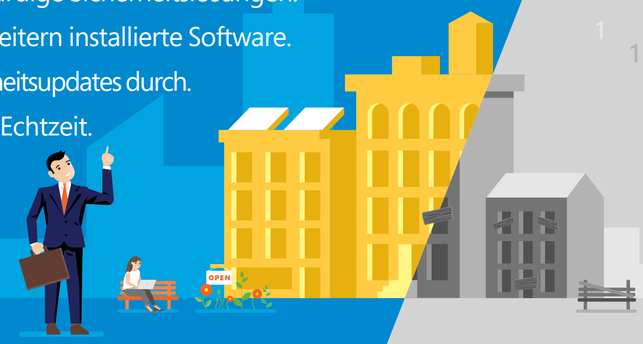
Device Guard

Smart Screen

Windows Defender

So vermeiden Sie Sicherheitsbedrohungen von raubkopierter Software:

- Beziehen Sie PCs und Software von vertrauenswürdigen Quellen.
- Vermeiden Sie unlizenzierte oder raubkopierte Software.
- Installieren Sie vertrauenswürdige Sicherheitslösungen.
- Überwachen Sie von Mitarbeitern installierte Software.
- Führen Sie regelmäßig Sicherheitsupdates durch.
- Sichern Sie Datendateien in Echtzeit.
- Zahlen Sie kein Lösegeld an Ransomware.



Geschäftskosten von Malware durch unlizenzierte Software

Über 10.000 $ **(in USD)**

pro infiziertem Computer*

Wahrscheinlichkeit einer Infektion durch raubkopierte Software aller Quellen?

28 %

Damit verursacht fast ein Drittel der unlizenzierten oder raubkopierten Software eine Malwareinfektion!

Größte Sorge der Unternehmen hinsichtlich Infektionen durch raubkopierte Software (n=202)

Verlust von Daten, Dateien und Unternehmensinformationen **59 %**

Aufwand und Kosten der Infektionsbeseitigung **41 %**

Systemausfälle **35 %**

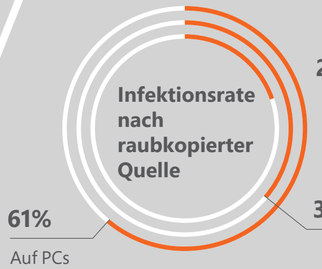
Verlust von geistigem Eigentum oder geschützten Informationen **28 %**

Nicht autorisierter Zugriff auf Daten **27 %**

Ransomware **23 %**

Schädigung des Unternehmensrufs **17 %**

Wo liegen die Ursachen?



Malware kann gefährliche Adware, Keylogger,Passwort-Diebe, Schlupflöcher für Hacker sowie Software enthalten, die Remotesteuerung von PCs ermöglicht.

Die Seiten, auf denen raubkopierte Software heruntergeladen wird, können Malware übertragen.

Drei Ursachen einer Infektion durch Malware

1 Software aus verdächtigen Quellen

33 % der Unternehmens-PCs wurden von nicht vertrauenswürdigen Quellen bezogen:

- **Auktionsseiten**
- **Onlineanbieter**
- **Berater**
- **PC-Hersteller**

2 Mitarbeitereigene Software auf Arbeitsgeräten

Eigene Software bei der Arbeit zu verwenden, kann den Anteil infizierter Software auf nternehmens-PCs um **19 % steigern.**

3 Nicht installierte Sicherheitsupdates

Die Gründe, aus denen Sicherheitsupdates nicht installiert werden, **reichen von der Angst,** mit raubkopierter Software aufzufliegen, bis hin zu fehlenden Updateprozessen und entsprechenden Kontrollen.

Über 66 % der Angriffe erfolgen, nachdem Updates zwar verfügbar waren, aber nicht installiert wurden.

Quelle: Ursachen und Kosten von Sicherheitsbedrohungen durch raubkopierte Software in Europa 2017. Veröffentlicht von IDC, September 2017.

**Softwaremanagement: Sicherheitsanforderung und Geschäftsgelegenheit. Globale BSA-Softwareumfrage, Juni 2018.*

*** Windows Hello mit spezieller biometrischer Hardware, z. B. einem Fingerabdruckleser, einem aktiven IR-Sensor oder anderen biometrischen Sensoren, erforderlich. Der hardwarebasierte Schutz von Windows Hello-Anmeldedaten/-Schlüsseln erfordert TPM 1.2 (oder höher). Wenn kein TPM vorhanden bzw. konfiguriert ist, sind Anmeldedaten/Schlüssel softwarebasiert.*

**** TPM-Schlüsselschutz erfordert TPM 1.2 (oder höher).*