

5 Netzübergänge absichern

ARGUMENTE:

Eine Firewall ist unverzichtbar. Ohne einen solchen Schutz sind Unternehmen völlig ungeschützt vor unerwünschten Zugriffen von außen.

Auch ohne besondere IT-Kenntnisse kann eine auf dem Arbeitsplatzrechner vorinstallierte Firewall aktiviert werden. Grundsätzlich sollte eine Firewall zentral konfiguriert werden. Dies ist bereits eine erste Schutzstufe gegen Angriffe. Die Verbindung von IT-Anwendungen mit dem Internet birgt eine Reihe von Risiken, dazu gehören Angriffe mit Ransomware, Datenexfiltration und Identitätsdiebstahl.

WEITERFÜHRENDE INFORMATIONEN:



FIREWALL

Eine lokale Firewall (entweder im Betriebssystem integriert oder als Softwarelösung eines Drittanbieters) sollte auf allen Arbeitsplatzrechnern installiert werden.

Darüber hinaus sollten auch kleine und mittlere Unternehmen vorrangig zentrale Firewalls (also spezielle Hardware) einsetzen, um die Verbindung zwischen Informationssystem und Internet zu schützen.

BSI – Cybersicherheit für KMU – Die TOP 14 Fragen, S. 18, Frage 8
<https://sl.csc-kmu.de/b5-01.html>



NETZÜBERGÄNGE IDENTIFIZIEREN UND SEGMENTIEREN

Verwenden Sie keine Gruppenaccounts, sondern für alle Beschäftigten ein eigenes Nutzerkonto. Normale Nutzende dürfen nicht über Administratorrechte verfügen.

Für das Navigieren im Internet dürfen nur eigene Benutzerkonten genutzt werden.

Dienstliche Computer sollten ausschließlich für die berufliche Arbeit genutzt werden.

BSI – Cybersicherheit für KMU – Die TOP 14 Fragen, S. 20-21, Frage 10
<https://sl.csc-kmu.de/b5-02.html>



CSBW-Factsheet: Netzkopplung und Fernzugriffe
<https://sl.csc-kmu.de/b5-03.html>

FALLBEISPIEL

Ein Planungsbüro mit fünf Mitarbeitenden hat in einem Router eine Portweiterleitung auf den Fileserver eingerichtet, damit die Mitarbeitenden von extern zugreifen können. Eine Firewall ist nicht vorhanden. Der Angriff erfolgte mit einem Verschlüsselungstrojaner. Da im Router ein Port offen war, konnten Angreifende auf den ungeschützten Fileserver zugreifen und alle Dateien verschlüsseln.

FOLGEN

Der Fileserver konnte mehrere Tage nicht genutzt werden. Die Daten konnten größtenteils über ein Backup wiederhergestellt werden.



**NOTFALLKONTAKT
CYBER-ERSTHILFE BW:**

0711-137-99999