

# Checkliste zur Cybersicherheit



## FÜR IHR SICHERHEITSKONZEPT



### Proaktives Monitoring

Um Risiken der Cyberkriminalität vorzubeugen, hilft eine proaktive Kontrolle und Überwachung Ihrer Unternehmens-IT. Der Einsatz intelligenter und früher Warnsysteme steigert die Sicherheit von Unternehmensdaten.



### IT-Security-Analyse

Bei immer komplexer werdenden IT-Infrastrukturen in Unternehmen entstehen Sicherheitslücken, die eine enorme Angriffsfläche für Hacker bieten. Das regelmäßige Prüfen der IT-Sicherheit im Unternehmen dient der Identifikation solcher Schwachstellen.



### Passwörter

Nicht nur das Anlegen sicherer Passwörter ist am Arbeitsplatz ein absolutes Muss. Um zu der IT-Sicherheit des Unternehmens zu gewährleisten, ist auch die regelmäßige Passwortänderung unverzichtbar.



### Patch-Management

Das Einspielen von Patches sorgt dafür, dass nach der Markteinführung von Software-Anwendungen erkannte Sicherheitslücken behoben werden. So werden Programmfehler beseitigt, um Malware-Angriffe abzuwehren.



### Human Firewall

Wie der Name bereits vermuten lässt, handelt es sich bei der Human Firewall um den menschlichen Abwehreinsetz am Arbeitsplatz: Damit ist die Sensibilisierung und Schulung von Mitarbeitern auf Cyberbedrohungen gemeint.



### Cloud Backup

Kein Sicherheitskonzept ohne Backup: Die Sicherung der Unternehmensdaten in einem Hochsicherheits-Rechenzentrum schützt nicht nur vor Datenverlusten, sondern auch vor unbefugten Zugriffen.

Sie haben Fragen zu den IT-Sicherheitsmaßnahmen?

➔ Besuchen Sie uns gerne auf [www.osite-network.de](http://www.osite-network.de)!