premium technologies

1. Technische Absicherung der IT-Infrastruktur Ihres Unternehmens

Um Schadsoftware und Angriffe von Ihrer IT fernzuhalten, gibt es verschiedene Maßnahmen:

Maßnahme	Schutzbereich	Erklärung
Firewall	Unternehmensnetzwerk	Schützt die komplette IT-Infrastruktur HINTER der Firewall vor direkten Netzwerkangriffen aus dem Internet oder auch eingeschleuster Schadsoftware
Unternehmensgeräte	Unternehmensnetzwerk	Verwenden Sie ausschließlich Geräte, die das Unternehmen stellt und verwaltet. Gerade im HomeOffice sollten keine Privat- oder Fremdgeräte verwendet werden! Das gilt auch für Smartphones.
Multi-Faktor-Authentifizierung	User / Geräte / Konten	Aktivieren Sie – wo möglich – die Multi-Faktor-Authentifizierung. Dies erhöht den Schutz vor Hacking und Phishing. Kann z. B. bei allen Microsoft 365, Amagno DMS oder Cloud-Produkten aktiviert werden.
Verschlüsselung	Geräte	Alle Geräte müssen verschlüsselt sein. So ist ein Zugriff auf Daten bei Diebstahl etc. nicht möglich.
Mobile Device Management	User / Geräte	Sobald Geräte mobil genutzt werden (Smartphone, Tablet, Notebook) solten diese verwaltet werden. So können die Geräte z. B. bei Verlust auch aus der Ferne gelöscht oder deaktiviert werden.
Datenspeicher	Unternehmensnetzwerk	Detaillierte Konzeption, wo Daten Ihres Unternehmens abgelegt werden. Vermeiden Sie ungeschützte Speicher wie USB-Sticks oder nicht-verwaltete Cloudspeicher. Zusätzlich sollte mindestens ein tägliches Backup aller Daten erfolgen.
Aktuelle Software	Unternehmensnetzwerk	Software immer auf dem aktuellen Update-Stand halten. Sollte es keine Updates für diese Version mehr gegeben auf eine aktuellere Version wechseln.
Geprüfte Software	Unternehmensnetzwerk	Installieren und nutzen Sie nur Software, welche geprüft ist und lassen Sie keine Installation aus unbekannten Quellen zu.

2. Organisatorische Maßnahmen

Neben den vorhandenen technischen Maßnahmen ist die Organisation von Prozessen und Abläufen ebenso sicher zu gestalten.

Maßnahme	Schutzbereich	Erklärung
Zugriffsbeschränkungen	Daten	Stellen Sie sicher, dass sowohl interne als auch externe Mitarbeiter nur zu den Daten Zugang haben, die auch benötigt werden. Darüber hinaus muss eine klare Passwortregelung und ein Berechtigungssystem vorliegen.
Alt-Geräte Entsorgung	Daten / Netzwerk	Geben Sie niemals alte Geräte weiter. Gerade im privaten Umfeld, bei Mitarbeitern oder Bekannten können Sie nicht nachvollziehen, ob noch vorhandene Daten auf den Geräten lesbar sind. Mindestens die Speicher der Geräte müssen physisch vernichtet werden.
Kommunikationswege	Unternehmen	Festlegung, welche Kommunikationswege geschäftlich genutzt werden. Dabei Ausschluss von nicht-verwaltbaren und ungeschützten Kanälen wie z. B. private Mailkonten oder Messenger (WhatsApp, Telegram etc.)
Checklisten und Belehrung	Unternehmen	Damit alle technischen und organisatorischen Maßnahmen auch greifen, müssen Ihre Mitarbeiter eine entsprechende Dokumentation und auch Leitfäden erhalten.
Verträge und Vereinbarungen	Unternehmen	Regeln Sie den Umgang mit IT-Geräten, Daten und vor allem Internet in Ihren Arbeitsverträgen. Vor allem bezüglich privater Nutzung, z. B. des Internets oder Speichermedien.
Externe Partner	Unternehmen	Prüfen Sie, ob – und wenn ja, welche – externen Partner Zugang zu Ihren Systemen haben oder Daten von Ihnen erhalten. Vereinbaren Sie mit diesen entsprechende Berechtigungen und Absicherungen.
Security Audit	Unternehmen	Prüfung aller Maßnahmen im Unternehmen und Erstellung einer Dokumentation mit allen vorhandenen und noch umzusetzenden Punkten. Danach sollte dieses jährlich wiederholt werden.

3. Sensibilisierung aller Nutzer

Einen guten Teil der IT-Sicherheit machen die Nutzer aus. Selbst bei optimal geschützten Systemen, können Nutzerfehler schwerwiegende Folgen haben. Daher empfehlen wir folgende Weiterbildungen.

Weiterbildung	Inhalt
Cybersecurity I	Trennung von privaten und geschäftlichen Daten - In vielen Unternehmen werden private Einkäufe oder Social Media über die Unternehmensaccounts gemacht. - Den Nutzern wird verdeutlicht, welches Risiko das ist und wie eine saubere Trennung zwischen Privat und Geschäft erfolgen kann und muss. - Wir erklären, welche Daten überhaupt interessant sind und über welche Wege wir diese (un)freiwillig preisgeben und wie das verhindert werden Kann.
Cybersecurity II	Persönliche und Unternehmensdaten schützen - Wir zeigen, wie jeder persönlich seine Daten (Geräte, Accounts, Konten) schützen kann und sollte. - Praktische Tipps für Passwort-Strategien - Nutzung von Multi-Faktor-Authentifizierung
Cybersecurity III	Angriffe erkennen und vermeiden - Wir erklären, welche Wege häufig verwendet werden, um Ihr Unternehmen anzugreifen. - Wir zeigen, wie man Angriffe (z. B. Fake-E-Mails) erkennen kann und wie jeder reagieren sollte. - Außerdem erklären wir, was zu tun ist, wenn der Verdacht eines erfolgreichen Angriffs besteht.

Wir bieten diese Kurse regelmäßig als offene Seminare an. Alternativ können Sie diese und andere Seminare individuell für Ihr Unternehmen buchen.

Alle Seminare werden bis auf weiteres per Microsoft Teams durchgeführt.

premium technologies

Grundlegende Informationen zur IT-Sicherheit – Checkliste für Nutzer

Anbei erhalten Sie eine Auflistung von grundlegenden Hinweisen zur Erhöhung der IT-Sicherheit in Ihrem Unternehmen. Die Liste ist keinesfalls abschließend.

Sichere Passwörter	Nutzen Sie am Arbeitsplatz und bei allen Konten (E-Mail, Shops etc.) sichere Kennwörter. Es sollten mindestens 8 Zeichen mit Buchstaben (Gross/Klein), Zahlen und Sonderzeichen sein. Nutzen Sie nach Möglichkeit kein Passwort doppelt.
eMail	Erhalten Sie E-Mails mit Anhängen oder Download-Links, prüfen Sie genau, ob diese E-Mail auch echt ist. Anhänge und Downloads wie z. B. *.zip oder *.doc können großen Schaden anrichten. Stellen Sie sich die Frage, ob Sie den Absender überhaupt kennen und wenn ja, ob er Ihnen Dateien auf diesem Wege schicken würde. Wenn Sie sich nicht sicher sind, fragen Sie Ihren IT-Administrator.
SMS / Messenger	Erhalten Sie auf Ihrem Smartphone SMS oder Nachrichten in anderen Messenger Diensten, welche einen Downloadlink enthalten, klicken Sie diesen nicht an. In 99 Prozent der Fälle sind es Fake-Nachrichten und der Download ist eine Schadsoftware.
Multi-Faktor-Authentifizierung	Wo möglich, nutzen Sie die Multi-Faktor-Authentifizierung. Hier müssen Sie beim Login noch zusätzlich einen Code aus einer SMS, App oder E-Mail eingeben, um zu bestätigen, dass Sie berechtigt sind. Das erhöht den Schutz der betreffenden Kontos erheblich.
Sichere Datenträger und Geräte	Wenn Sie externe Speichermedien (z. B. USB-Sticks) nutzen, prüfen Sie, ob diese verschlüsselt sind. Bei Verlust eines unverschlüsselten Speichers sind alle Daten offen zugänglich. Ebenso betrifft dies mobile Geräte wie Notebooks oder Tablets.
Arbeitsplatz sperren	Sperren Sie Ihren PC wenn Sie Ihren Arbeitsplatz verlassen. Dies kann z. B. schnell per Tastatur mit  geschehen. So kann während Ihrer Abwesenheit niemand unberechtigt Informationen von Ihrem Rechner entwenden.
Schutz-Reaktion	Trotz aller Sorgfalt kann immer etwas passieren. Sollten Sie feststellen, dass eine Schadsoftware auf Ihrem Rechner ist, Sie gehackt wurden oder auch nur bemerken, dass Ihr Rechner sonderbare Dinge tut – Schalten Sie sofort den Rechner aus und informieren Sie den IT-Administrator. Je schneller, desto besser.