CHECKLISTE

Ihre IT-Security

Wie sicher ist Ihre IT-Umgebung wirklich? Cyberkriminalität ist noch immer auf dem Vormarsch und eine Bedrohung für jeden! Ein durchdachter IT-Notfallplan ist der gute erste Schritt, um Ihr Unternehmen auf sichere Beine zu stellen. Damit Ihr Unternehmen aber auch langfristig sicher bleibt, sind weitere Maßnahmen gefragt.

Beantworten Sie diese 15 Fragen, um zu verstehen, wie sicher Ihre IT-Umgebung ist und welche Maßnahmen noch erforderlich sind.

	Frage	Ja	Nein	Unklar
1.	Haben Sie einen Überblick über die aktuell eingesetzte Software und deren Versionen auf allen Rechnern in Ihrem Unternehmen? Sind die Daten in Ihrer Infrastrukturanalyse noch aktuell?	○	○	○
2.	Liegt Ihnen ein aktueller und detaillierter Plan Ihrer Netzwerkstruktur und eine Auflistung der eingesetzten Hard- und Software in Ihrem Netzwerk vor? (Netzwerkdokumentation)	○	○	○
3.	Arbeiten Sie ausschließlich mit Windows 10 oder höher?	○	○	○
4.	Ist auf Ihren Servern Microsoft Server 2016 oder höher installiert? Ist ein eventuell verwendetes Linux aktuell?	○	○	○
5.	Sind Sie sicher, dass Ihre Computer tagesaktuell mit Sicherheitsupdates versorgt werden? Manuell oder automatisiert? (Betriebssystem, Exchange OnPrem, Internet-Browser, Office, Adobe Reader usw.)	○	○	○
6.	Sind die Antiviren-Programme auf all Ihren Firmen-Geräten stets aktuell und überwacht – auf Smartphones, Notebooks und Tablets? (Antivirus Management, Mobile Device Management)	○	○	○
7.	Ist die Internetverbindung Ihrer Firmen-Geräte und Server durch eine jederzeit aktuelle Firewall geschützt? (Firewall Management, Mobile Device Management)	○	○	○
8.	Verfügt Ihr Unternehmen über ein systematisches und getestetes Verteilen von Sicherheits-updates und Funktionsupdates auf allen genutzten Geräten? Werden die Updates vor dem Verteilen auf „unerwünschte Nebenwirkungen“ getestet? (Patch Management)	○	○	○
9.	Ist die Verbindung sensibler IT-Systeme von anderen IT-Bereichen in Ihrem Netzwerk getrennt, um bspw. die Ausbreitung von Schadsoftware in Ihrem Netzwerk zu unterbinden? (Netzwerksegmentierung)	○	○	○
10.	Werden Ihre wichtigen und steuerrelevanten Unterlagen regelmäßig aktualisiert, strukturiert verwaltet und sicher abgelegt sowie rechtskonform archiviert? (Backup Management, GoBD, DSGVO)	○	○	○
11.	Haben Sie eine Datensicherung eingerichtet? Schützt Sie diese vor Unfällen wie Bränden, Überschwemmungen o.ä.?	○	○	○
12.	Verfügen Sie über einen IT-Notfallplan zur Datenwiederherstellung nach einem Systemausfall? (Disaster Recovery)	○	○	○
13.	Gibt es bei Ihnen ein Rechtemanagement, das sicherstellt, dass nur die Mitarbeiter Administratorenrechte besitzen, die diese zwingend benötigen?	○	○	○
14.	Setzen Sie eine Zwei-Faktor-Authentifizierung zur Extra-Absicherung von Zugängen überall dort ein, wo sie verfügbar ist?	○	○	○
15.	Sind Ihre Mitarbeiter zu den Themen Phishing und Spam geschult?	○	○	○

Mehr Informationen gefällig?

TB-Computer IT-Systemhaus | Telefon: 0211 7606559
info@tbcomputer.de | www.tbcomputer.de

06.2024