



Cybersicherheit für KMU

Die Essenz für Ihr Überleben im digitalen Zeitalter

Bei IT-Security gilt: Vorsicht ist besser als Nachsicht. Einmal gehackt, laufen die Kosten und Schäden oft ins Unermessliche. Genau dafür sind wir von der xinfra gmbh für Sie da. Wir bieten praxiserprobte IT-Lösungen für KMU, analysieren zusammen mit Ihnen Ihre bestehende IT-Infrastruktur, decken Schwachstellen auf, beheben diese und stellen sicher, dass Ihr Unternehmen über die beste Abwehrstruktur verfügt.

Setzen Sie die Hürde für Cyber-Kriminelle so hoch, dass Sie nicht erpressbar sind.

Swiss Cyber Defence DNA (SCD-DNA) ist ein Leitfaden für Ihr KMU, mit dem Sie sich einfach und effizient gegen Gefahren der Cyber-Kriminalität und grossem finanziellen Schaden schützen können.

xinfra ist Umsetzungspartner der SCD-DNA, einer Initiative der MOUNT10 AG unter Mitwirkung verschiedener Industriepartner. Weitere Informationen finden Sie auf scd-dna.ch oder xinfra.ch.



Massnahme Nr. 1 - Aktuelle unveränderbare Datensicherung / schreibgeschütztes Backup

Ihre Überlebensfähigkeit als Firma sichern, ähnlich dem Airbag im Auto

- Eine Person für die Umsetzung und Überprüfung definieren
- Externe Speicherung des Backups sicherstellen
- Automatisierter, schreibgeschützter Backup-Prozess inkl. Verschlüsselung
- Wenn obiges nicht möglich: Backup-Medium vom Netzwerk trennen und offline lagern

Massnahme Nr. 2 - Umfassender und aktueller Schutz vor Schadsoftware

Dies ist Ihre erste Verteidigungslinie, wie eine sichere Haustüre

- Sensibilisierung und Schulung von Mitarbeitern im Umgang mit Emails, Webseiten, Passwörtern etc.
- Umfassender, flächendeckender Malwareschutz von Endgeräten, Servern, Cloud- und E-Mail Services
- Makroausführung einschränken; Internet- und Spamfilter installieren

Massnahme Nr. 3 - Netzwerke und Fernzugriffe absichern

Ihre Verteidigungsabschnitte für eine selektive Unterbindung nicht-autorisierter Zugriffe

- Schulung der Mitarbeiter und Lieferanten für Fernzugriff
- Netzwerke mittels Firewall in Zonen aufteilen, damit wichtige Geschäftsbereiche voneinander abgeschottet sind
- Fernzugriff mittels 2-Faktoren Authentifizierung zusätzlich absichern (z.B. SMS Code)

Massnahme Nr. 4 - Hardware und Software aktuell halten

Ihre Garantie für eine sichere, funktionierende IT

- Eine Person definieren, die für die Verwaltung und periodische Überprüfung der Lizenzen / Updates verantwortlich ist
- Gemäss Risikobeurteilung veraltete Systeme ablösen und bestehende physisch schützen (z.B. Zutritt zum Server)
- Nur aktuelle Betriebssysteme und Applikationen einsetzen
- Alte Systeme vom Netzwerk isolieren

Massnahme Nr. 5 - Mitarbeiter und deren Rollen

Ihr Selbstschutz mittels Einschränkung auf das Notwendige

- In einem Rollenkonzept definieren, welche Rechte pro Mitarbeiter notwendig sind
- Zugriffsrechte der Geschäftsleitung ebenfalls prüfen und einschränken
- Passwortregeln für Mitarbeitende erstellen
- Definierte Rollen mit den Zugriffsrechten koppeln und einschränken

Massnahme Nr. 6 - Notfallprozesse definieren

Ihre Absicherung in der Not mittels klar definiertem Plan anstelle von Improvisation

- Notfall-Organisation bestimmen, Prozesse definieren und alle Mitarbeiter informieren
- Rollen und Abläufe regelmässig überprüfen und Datenrückführung testen
- Unabhängige Technologie nutzen, um auch im Notfall auf die Dokumente zugreifen zu können (z.B. Notfall-Zettel, Ordner, Cloud oder Mobile Lösung)

Noch unsicher? Unsere Cybersecurity-Experten beraten Sie gerne, um die optimale Cybersicherheit für Ihre Bedürfnisse zu evaluieren.