Informationssicherheit – 10 Sofortmassnahmen	Massnahmen	Denkanstösse
1. Verantwortlichkeiten	• Verantwortlichkeit definieren, inkl. Budget (GL-Ebene) • Externe Dienstleister einbinden und überprüfen • Regelmässige Weiterbildung und Reportings	Informationssicherheit ist Chefsache – spätestens wenn das Unternehmen stillsteht. Verträge mit Dienstleistern schliessen und überprüfen.
2. Backup und Wiederherstellung	• Backupkonzept verschriftlichen • Überprüfen ob die „Recovery Time“ tragbar ist • Regelmässige Restore Tests	Lebensversicherung eines KMU! Ob das Backup wirklich funktioniert, sieht man erst beim erfolgreichen Restore. 3-2-1 Regel beachten.
3. Identity & Access	• Zugriffsrechte definieren und überprüfen (insbesondere Admins) • Passwortmanager und Multifaktorauthentifizierung • Sichere externe Zugriffe	Bildschirmsperre bei Inaktivität, Remote-Zugriffe, Zugriffsberechtigungen, Persönliche Accounts, Multifaktorauthentifizierung, VPN bzw. Verschlüsselung
4. Regelmässige Updates	• Sicherheitsupdates zeitnahe installieren, besonders beim Antivirus • Wo möglich Updates automatisch installieren • Lifecycle berücksichtigen und alte Systeme ablösen	Im Idealfall werden kritische Schwachstellen (CVE) überwacht
5. Sensibilisierung und Schulung	• Schulungen zur IT-Sicherheit • Phishing-Simulationen	Die meisten Angriffe starten mit einer E-Mail welches einen Link oder Anhang enthält.
6. Notfallplan	• Wichtigste Systeme identifizieren und priorisieren • Interne und externe Kontakte auf Papier im Safe • IT-Dokumentation inkl. Passwörter auf Papier im Safe	Ein definiertes Incident-Response-Team kann bei einem Notfall wie z.B. einer Ransomware-Attacke die Reaktionszeit stark reduzieren.
7. Netzwerk-Segmentierung	• WLAN Intern & Gast separieren (BYOD für Mitarbeiter) • Verschiedene Netzwerke erstellen • Diagnosegeräte möglichst in separates Netzwerk	Sensible Daten und Systeme sollten in separaten Netzwerken isoliert werden, um das Risiko von Datenlecks zu minimieren.
8. Daten-vernichtung	• Entsorgung von Papierunterlagen und Datenträger • Austrittsprozess definieren • Daten von Occasion- & Servicefahrzeuge von ehem. Kunde löschen	Zertifizierte Vernichtungsdienste entsorgen Altpapier und alte elektr. Speichermedien fachgerecht. Was man nicht hat, kann man nicht verlieren.
9. Anwendungs-kontrolle	• Eingeschränkte Installationsrechte für Mitarbeitende • IT-Inventar erstellen für Endgeräte (mobil & statisch) sowie Appl. • Gemeinsame Benutzerkonten vermeiden	Sind Gefahren wie Office-Makros bekannt? Gemeinsame Accounts vermeiden, da ehemalige Mitarbeiter immer noch auf Daten zugreifen können.
10. Cyber-versicherung	• Schutz vor finanziellen Schäden • Auslagern des Know-Hows, falls kein Fachwissen in der Firma • Katalog der Cyberversicherung zeigt der Basis-Schutz schon auf	Wiederherstellungskosten, Betriebsunterbrechung und Erpressung durch Ransomware.
Bussgelder und Schadenersatz bei Sicherheitsverletzung	• DSG Art. 8 i.Vm. Art. 61 lit. c Verletzung der Informationssicherheit; **Strafverfahren mit Bussgeld** von bis zu CHF 250‘000 • OR Art. 754 **Schadenersatzhaftung** der Geschäftsführer/des Verwaltungsrates gegenüber den Aktionären/Eigentümern für absichtlich oder fahrlässige Pflichtverletzung.	

Aufzeichnung mit Erfahrungsbericht zu Hackerangriff

Informationssicherheit – 10 Sofortmassnahmen für Garagen! ; 3. Juli 2024;
Autoren: Impunix AG – Micha Strässler & Leo Krähenbühl - info@impunix.ch

impunix datenschutz full-service