ALBERT KOECHLIN STIFTUNG

DIGITALISIERUNG NPO: DATEN-SICHERHEIT

Unternehmen werden immer öfters von Cyberkriminelle angegriffen. Vor Angriffen sind auch Nonprofit-Organisationen nicht gefeit, insbesonders, da NPOs oft über weniger Schutzmechanismen verfügen, um ihre Systeme oder ihre Daten zu sichern.

Die IT-Sicherheit lässt sich auch mit geringen Ressourcen erhöhen. Eine ausführliche Übersicht über Risiken und Handlungsmöglichkeiten bietet das «Nationale Zentrum für Cybersicherheit (NCSC)» unter **https://www.ncsc.admin.ch/.**

Acht Tipps aus dem Alltag

1. Verantwortlichkeiten wahrnehmen, Risiken erkennen
   Die Verantwortung für die IT-Sicherheit gehört in die oberste Führungsetage. Welche Auswirkungen hat der Ausfall der IT oder der Verlust von Daten? Eine 100%-IT-Sicherheit gibt es nicht.

   Proaktiv ist besser als reaktiv:
   → SecurityCheck machen, Löcher schliessen;
   → Worst-Case Planen (Welche IT-Infrastruktur und in welcher Reihenfolge muss nach einem Schadenfall wieder laufen, verfügbar sein / wie wird wann und wer informiert / gibt es einen Notfallplan → Stecker ziehen)
   → Klassifizieren der Daten (Welche Daten sind unverzichtbar? / Auf welche Daten kann ich bei einem Wiederherstellungsfall verzichten?)

2. Mitarbeitende sensibilisieren
   Der Sensibilisierung der Mitarbeitenden im Umgang mit der IT-Infrastruktur und mit Gefahren der digitalen Welt ist zentral. Oft ist menschliches (Fehl-)Verhalten der Ursprung für einen Sicherheitsvorfall. Nach aktuellen Studien ist der Faktor Mensch das grösste Sicherheitsrisiko.

3. Virenschutz, Software und Betriebssysteme laufend aktualisieren
   - Auf jedem Computer muss ein Virenschutz installiert sein und dieser muss regelmässig aktualisiert werden. Wichtig sind regelmässige, (z.B.: monatliche) vollständige Systemscans;
   - Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware. Auf allen Computern, Servern und der Hardware (Drucker, Router, …) sollen Sicherheitsupdates automatisch eingespielt werden oder auf aktuellen Stand gehalten werden. Die Firmware ist ebenfalls laufend zu aktuallisieren.

4. Offline-Backups der Daten erstellen, speichern und testen
   - Regelmässig/automatisch Backups (Sicherheitskopien) ihrer Daten (z.B.: auf einer externen Festplatte oder einem NAS (netzgebundener Speicher)) erstellen;
   - Regelmässig prüfen, ob das Backup funktioniert und auch wirklich die Daten gespeichert werden;
   - Offline-Backups (Sicherheitskopien werden vom Computer getrennt) damit diese Daten bei einem Ransomware-Angriff (Daten werden durch Dritte verschlüsselt) nicht auch mitverschlüsselt werden;
   - Eine Kopie der Daten extern aufbewahren (Datenwiederherstellung nach Brandfall, …) und regelmässig ersetzen;
   - Auch Daten auf Online-Speichern regelmässig sicher (Online mit Versionierung / Offline auf externen Festplatten (Daten verschlüsseln):

5. Netzwerke und Computer schützen
   - Jeder PC mit einer Firewall schützen (Software). Zusätzlich das Unternehmensnetzwerk mit einer physischen Firewall (UTM-Dienste, Content-Filter) gegen Zugriffe von aussen schützen;

- Auf mobilen Geräten den BitLocker von Microsoft aktivieren. Der BitLocker verschlüsselt die Festplatte, somit können auf gestohlenen Geräten keine Daten ausgelesen werden;
- Fernzugriffe auf das Unternehmensnetzwerk (Home-Office) nur über ein virtuelles privates Netzwerk (VPN) zulassen, wobei der Zugriff durch eine Zwei-Weg-Authentifizierung geschützt wird.

  → Sicherer Umgang mit Fernzugriffen (Infos ncsn)

6. Passwörter und Authentifizierungsmethoden
   - Passwörter nicht mehrfach verwenden und für jeden einzelnen Onlinedienst ein anderes Passwort verwenden. Passwort-Manager helfen den Überblick zu behalten;
   - Passwörter sollten mindestens 12 Zeichen lang sein und aus Klein-, Grossbuchstaben, Zahlen und Sonderzeichen bestehen;
   - Der Zugang zu Internet- und Clouddienste mit einer Zwei-Faktor-Authentifizierung absichern;
   - Mittels «Pishing» versuche Kriminelle an Passwörter zu kommen. Passwörter dürfen nie auf Internetseiten eingegeben werden, welche über einen Link geöffnet wurden (z.B.: Aufforderung zur Passworteingabe via Email). Banken, Telefon, Gepäckdienste und weitere Dienstleister fragen nie nach einem Passwort via Email oder Telefon;
   - Standardpasswörter bei der Installation sofort ändern (Drucker, Router, Firewall, ….);
   - Passwörter regelmässig zu ändern wird nicht mehr empfohlen. Ein gutes Passwort, kann man bedenkenlos über mehrere Jahre hinweg nutzten. Das regelmässige Ändern führt eher dazu, dass ein schwaches Passwort benutzt wird;

     → Artikel auf heise.de «Passwörter: BSI verabschiedet sich vom präventiven, regelmässigen Passwort-Wechsel»

     → Schützen sie Ihre Konten / Passwörter (Infos ncsn)

     → Verhalten bei E-Mail (Infos ncsn)

7. Zahlungen
   - Zahlungen nur Einhaltung des Vier-Augen-Prinzipes auslösen. Auch unter Zeitdruck oder bei «dringenden» Zahlungsaufträgen intern nachfragen, ob die Zahlung berechtig ist;
   - Zahlungen nie an «öffentlichen» Geräten ausführen (z.B. Internetcafe) oder in öffentlichen Netzwerken (PublicWLANs wie am Flughafen, im Bahnhof, …);

   → CEO-Betrug (Infos ncsn)

   → E-Banking Schadsoftware (Infos ncsn)

8. Unterstützung holen

   Der beste Weg, IT-Gefahren zu begegnen, ist die Zusammenarbeit mit entsprechenden Experten (Schulung von Mitarbeitenden, Definition von Sicherheitsrichtlinien, Sicherheitstest, Schutz der Computer und Netzwerke).

17.1.2021/pwc