ALBERT KOECHLIN STIFTUNG

DIGITALISIERUNG NPO: VERBESSERUNG DER DATENSICHERHEIT

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.

Beispiele, um mit geringem Aufwand die Sicherheit zu erhöhen

1. Einbau physischer Firewall ins Netzwerk
   Eine **Firewall** (von englisch firewall ‚Brandwand' oder ‚Brandmauer') ist ein Sicherungssystem, das ein internes Netzwerk oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.

   Die Firewall überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden.

   Nebst den auf den einzelnen Computern installierten Firewalls empfiehlt sich das interne Netzwerk mit einer externen, physischen Firewall (auch Netzwerk- oder Hardware-Firewall) zusätzlich zu schützen.

2. Mehrfache Datenspeicherung inkl. einem Offline-Backup
   Die einfachste Möglichkeit, Daten vor bösartigen Zugriffen zu schützen, besteht in einem Offline-Backup, d. h. einem Backup, bei dem die Speichermedien getrennt von der bestehenden IT-Infrastruktur aufbewahrt werden. Offline-Backups bieten eine hohe Sicherheit gegenüber externen Zugriffen. Im Alltag haben sich mehrstufige Sicherungssysteme bewährt:

   a. 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;
   b. Zusätzlich wöchentlich ein Offline-Backups (Sicherheitskopien werden nach dem Backup vom Computer getrennt) erstellen. Diese Daten können bei einem Ransomware-Angriff (Daten werden durch Dritte verschlüsselt) nicht auch mitverschlüsselt werden. Die Daten können auf externen Festplatten oder Magnetbänder aufbewahrt werden;
   c. Eine Kopie der Daten extern (in Banksafe, beim Geschäftsführer:in zu Hause) aufbewahren (Datenwiederherstellung nach Brandfall, …) und regelmässig (monatlich) ersetzen.

06.01.2022/pwc