

Cyberangriffe verhindern

Tipps für Unternehmungen

Ein Cyberangriff kann jedes Unternehmen treffen. Mit einigen Vorsichtsmassnahmen können Sie sich jedoch schützen. Hier geben wir Ihnen einige Tipps, mit welchen Sie die Sicherheit Ihrer Unternehmung massgeblich erhöhen können.

Datensicherung

- Definieren Sie einen Prozess, der die regelmässige Datensicherung regelt.
- Überlegen Sie sich, wie viele Tage Datenverlust Sie verkraften können. Lagern Sie eine Kopie Ihres Back-ups zusätzlich getrennt (offline) und ausser Haus (offsite) aus.
- Stellen Sie sicher, dass Sie Vorgängerversionen des Back-ups über einen mehrmonatigen Zeitraum aufbewahren.

Umgang mit Informationen

- Überlegen Sie genau, welche Informationen Sie zum Beispiel auf Ihrer Webseite oder in sozialen Medien offenlegen.
- Über anonyme Kanäle wie Telefon oder E-Mail sollten grundsätzlich keine vertraulichen Informationen weitergegeben werden.

Umgang mit E-Mails

- Seien Sie misstrauisch bei Links oder Anlagen in E-Mails unbekannter Absender/innen.
- Scheuen Sie sich nicht vor persönlichen Rückfragen, wenn Ihnen etwas ungewöhnlich vorkommt und mahnen Sie Ihre Mitarbeitenden zur entsprechenden Vorsicht.

Sichere Passwörter

- Die Mindestlänge des Passwortes sollte bei mindestens zwölf Zeichen liegen und sowohl aus Buchstaben, Zahlen wie auch Sonderzeichen bestehen.
- Setzen Sie, wo immer möglich, auf eine Zwei-Faktor-Authentifizierung.

- Vermeiden Sie unbedingt die Mehrfachverwendung von gleichen Passwörtern. Benutzen Sie stattdessen einen Passwortmanager und generieren für jede Anwendung ein eigenes Passwort.
- Nutzen Sie einen Passwort-Manager.

Zugriffsschutz auf Daten

- Mitarbeitende sollten standardmässig über keine Administratorenrechte verfügen.

Zahlungen über einen separaten Computer

- Für Zahlungen sollten Sie einen separaten Computer benutzen, auf dem Sie nicht im Internet surfen oder E-Mails empfangen.
- Regeln Sie die Prozesse, die den Zahlungsverkehr betreffen (z.B. Vier-Augen-Prinzip und Kollektivunterschrift) und sprechen Sie mit Ihrer Bank über Sicherheitsmassnahmen.

Sicherheitsupdates

- Stellen Sie sicher, dass sämtliche Computer und Server in Ihrem Netzwerk Sicherheitsupdates automatisch einspielen.

Netzwerk schützen

- Auf jedem Computer sollten Sie eine Personal Firewall verwenden. Schützen Sie zudem Ihr Unternehmensnetzwerk mit einer Firewall vor dem Internet.
- Unterteilen Sie Ihr Unternehmensnetz in einzelne Bereiche, wie zum Beispiel für Produktion, Personal und Buchhaltung. Schützen Sie Fernzugriffe auf Ihr Netzwerk mit einer Zwei-Faktor-Authentifizierung oder setzen Sie eine sicherere Verbindung über ein virtuelles privates Netzwerk (VPN) ein.

Die Luzerner Polizei beantwortet gerne Ihre Fragen.



117 POLIZEI-NOTRUF