Zehn Tipps, um Cyberangriffe zu verhindern

Ein Cyberangriff kann jedes Unternehmen treffen. Mit einigen Vorsichtsmassnahmen können Sie sich jedoch schützen.

Sichern Sie Ihre Daten
Definieren Sie einen Prozess, der die regelmässige Datensicherung regelt. Überlegen Sie sich, wie viele Tage Datenverlust Sie verkraften können, und lagern Sie entsprechend 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.

Regeln Sie den Umgang mit Unternehmensinformationen
Überlegen Sie genau, welche Informationen Sie zum Beispiel auf der eigenen Website oder in sozialen Medien offenlegen. Über anonyme Kanäle wie Telefon oder E-Mail sollten grundsätzlich keine vertraulichen Informationen weitergegeben werden.

Sensibilisieren Sie Ihre Mitarbeitenden im 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.

Verwenden Sie sichere Passwörter
Die Mindestlänge des Passwortes sollte bei zwölf Zeichen liegen und sowohl aus Buchstaben, Zahlen wie auch Sonderzeichen bestehen. Setzen Sie wo immer möglich auf eine Zwei-Faktor-Authentisierung. Vermeiden Sie unbedingt die Mehrfachverwendung von gleichen Passwörtern! Stattdessen benutzen Sie einen Passwortmanager und generieren für jede Anwendung ein eigenes Passwort.

Regeln Sie den Zugriffsschutz auf Daten
Mitarbeitende sollten standardmässig über keine Administratorenrechte verfügen.

Verwenden Sie für Zahlungen 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 (zum Beispiel Vier-Augen-Prinzip und Kollektivunterschrift) und sprechen Sie mit Ihrer Bank über mögliche Sicherheitsmassnahmen.

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

Schützen Sie Ihr Netzwerk
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. Es gibt keinen Grund, weshalb Mitarbeitende des Personaldienstes auf Ihre Produktionsanlage zugreifen sollten.

Schützen Sie Fernzugriffe auf Ihr Netzwerk mit einer Zwei-Faktor-Authentisierung oder setzen Sie eine sicherere Verbindung über ein virtuelles privates Netzwerk (VPN) ein.

Installieren Sie einen Virenschutz
Stellen Sie sicher, dass auf jedem Computer ein Virenschutz installiert und der Echtzeitschutz aktiviert ist.

Vorsichtiger Umgang mit Clouddiensten
Sensible Daten und Firmengeheimnisse sollten nie unverschlüsselt in der Cloud abgelegt werden.

Details zu den Massnahmen finden Sie in unserer Broschüre «Cyberdelikte verhindern, Wegleitung für kleine und mittlere Unternehmen» oder auf www.melani.admin.ch

In Zusammenarbeit mit der Kantonspolizei Bern und MELANI