Zürcher Kantonalbank

Schutz vor Cyberkriminalität

Wichtigste Massnahmen und nützliche Links

Firewall
Eine Firewall überwacht den eingehenden und ausgehenden Netzwerkverkehr und entscheidet anhand von definierten Regeln, ob der Datenverkehr zugelassen oder blockiert wird.

Antiviren-Software
Neue Schadsoftware entsteht fast stündlich. Um diese rechtzeitig zu erkennen, empfiehlt sich der Einsatz einer Antiviren-Software. Diese sollte sich automatisch aktualisieren und mit einem Passwortschutz versehen sein. Installieren Sie keinesfalls mehrere Antiviren-Software gleichzeitig. Diese könnten sich gegenseitig neutralisieren.

Log Management System
Ein Log Management System ermöglicht einem Administrator zu prüfen, ob ein Angreifer unbemerkt in ein Computersystem eindringen konnte. Dabei werden Logfiles aus diversen Applikationen gesammelt und korreliert. Intelligente Auswertungsfunktionen helfen dabei, die gewünschte Information auf einfache Weise zu finden.

Intrusion Detection System
Ein Intrusion Detection System erkennt aufgrund von anpassbaren, definierten Regeln Angriffe auf Computersysteme oder Netzwerke. Die eingebaute Alarmierungsfunktion informiert den Administrator umgehend über den Eindringversuch, damit entsprechende Gegenmassnahmen eingeleitet werden können.

Sicherheitsupdates
Sämtliche auf dem Computersystem installierte Software muss stets aktuell gehalten werden. Damit wird verhindert, dass sich Schadsoftware über Lücken in den installierten Applikationen verbreiten kann. Falls vorhanden, sollte die automatische Updatefunktion der Software eingeschaltet werden.

Privilegierte Benutzeraccounts
Benutzer mit Administratorenrechten oder Benutzer mit erhöhten Rechten stellen ein Risiko für das Unternehmen dar, da sie oft von Cyberkriminellen ausgenutzt werden. Administratorenrechte sollten daher äusserst restriktiv vergeben werden. Zudem sind derartige Benutzeraccounts besonders zu überwachen.

Content-Filter
Benutzer greifen täglich auf das Internet zu, um ihre Arbeit erledigen zu können. Ein Content-Filter überwacht den Internet-Verkehr und blockiert schädlichen Inhalt oder schädliche Webseiten, bevor diese auf dem Arbeitsplatz des Benutzers ausgeführt werden.

Passwort-Sicherheit
Das regelmässige Ändern des Passwortes bringt sicherheitstechnisch gesehen keinen Mehrwert. Oft verwenden Benutzer Zahlen im Passwort, welche bei einem Passwortwechsel hochgezählt werden. Dies reduziert die Sicherheit. Anstelle dessen sollte für jede Applikation und für jede Webseite ein unterschiedliches Passwort verwendet werden, welches mittels Passwort-Generator erstellt wurde. Diese eignen sich zudem auch um die Passwörter sicher aufzubewahren.

Nützliche Links

Meldeformular für Unternehmen (Nationales Zentrum für Cybersicherheit NCSC)
https://www.ncsc.admin.ch/

SSL Server Test:
https://www.ssllabs.com/ssltest/

Passwort-Sicherheit überprüfen:
https://haveibeenpwned.com/

Cybersecurity Schnelltest:
https://ictswitzerland.ch/themen/cyber-security/check/offline-check/

Browser härten:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/SicherheitsCheck/sicherheitscheck_node.html

Information zu allgemeinen IT-Risiken:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/risiken_node.html

Tipps für sicheres eBanking:
https://www.ebas.ch/