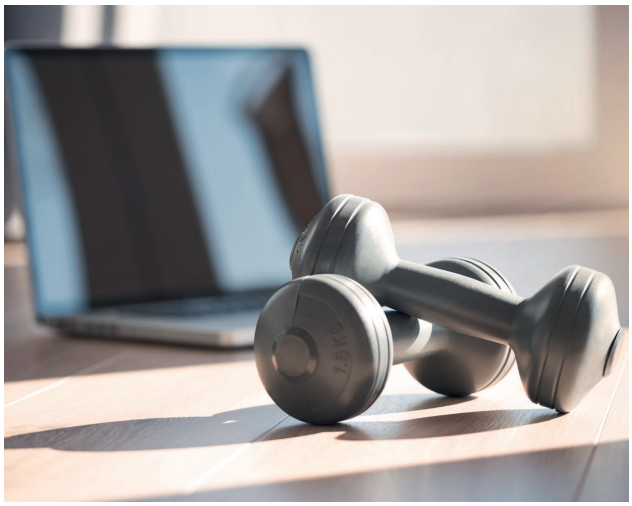
Cyberkriminelle setzen auf die Schwachstelle Mensch

Die Cyberkriminalität nimmt rasant zu und dabei greifen Hacker meist über die grösste Schwachstelle an: den Menschen. Aktuelle Befragungen zeigen, dass Institutionen im Zusammenhang mit der Corona-Pandemie und der Einführung des elektronischen Patientendossiers (EPD) digitaler werden, jedoch die daraus resultierenden Cyberrisiken unterschätzen. Zudem fehlen häufig Notfallpläne und oftmals auch das Bewusstsein, dass die eigene Institution Ziel eines Cyberangriffs sein kann.



Die häufigsten Angriffsstrategien

Die einfachsten Einfallstore für Cyberkriminelle sind Unwissenheit, Nachlässigkeit oder Neugier des Anwenders – und die Technik dazu, beispielsweise Phishing, Baiting oder Social Engineering Fraud.

Bei Phishing und Baiting wird die Unwissenheit der Mitarbeitenden ausgenutzt. So wurden kürzlich gefälschte E-Mails von Microsoft verschickt, die täuschend echt aussehen. Sie verleiten dazu, sich in das persönliche Microsoft-Konto einzuloggen. Baiting (zu Deutsch «Ködern») kommt oft als vermeintlicher Gewinn daher. Schnell folgt die Aufforderung zur Eingabe von Anmeldedaten. Die Eingabemaske ist bei beiden Varianten gefälscht und die Angreifer zeichnen die Angaben auf. Bei Social Engineering Fraud werden Mitarbeitende mit Täuschung oder Druck dazu aufgefordert, die üblichen Kontrollmassnahmen zu umgehen und sensible Daten preiszugeben oder Transaktionen auszulösen.

Diese Angriffsmethoden funktionieren nur, weil viele Mitarbeitende nicht das Wissen haben, Betrugsversuche durch Cyberkriminelle von echten geschäftlichen E-Mails zu unterscheiden. Stossen die technischen Möglichkeiten an ihre Grenzen, gefährliche E-Mails von den Postfächern fernzuhalten, steht nur noch die Person vor dem Bildschirm als Verteidigung zwischen den Kriminellen und der Institution. Daher sollte jede Institution Mitarbeitende für das Thema sensibilisieren und schulen.

Cyberversicherungen und Cybertraining

Der beste Schutz ist, auf alle Komponenten zu setzen: Eine bedarfsgerechte technische Verteidigung, eine geschulte «menschliche Firewall» und eine Versicherungslösung, die im Falle eines Versagens der Verteidigung die Kosten des Schadens deckt und hilft, das Schadensausmass so gering wie möglich zu halten. Für den Abschluss einer Cyber-Versicherung werden immer höhere Anforderungen an die Cyberfitness von Institutionen und deren Mitarbeitenden gestellt. Die Partner des Versicherungsdienstes von CURAVIVA Schweiz unterstützen und beraten Institutionen gerne in diesem Zusammenhang.

Cyberfitness für die Mitarbeitenden

Funk CyberAware deckt die wesentlichen Trainings- und Sensibilisierungsbedürfnisse ab. Die Trainingsprogramme stehen virtuell zur Verfügung und sind somit auch in der aktuellen Homeoffice-Zeit einfach einsetzbar. Funk stellt nebst den Programmen auch die Durchführung, die Koordination und die Administration sicher. Der Wissensstand der Mitarbeitenden kann in Reports abgebildet werden. Damit lassen sich Stärken und Schwächen der Belegschaft ermitteln und anschliessend gezielt angehen – und dies mit minimalem Aufwand seitens des Arbeitgebers. Weitere Informationen finden Sie unter www.funk-gruppe.ch/cyberaware.

Partner

neutrass
Versicherungen · Vorsorge · Finanzen

NEUTRASS-RESIDENZ AG
Herr Pirmin Lang
6343 Rotkreuz
Tel. 041 799 80 49
pirmin.lang@neutrass.ch

Funk Insurance Brokers AG
Herr Simon Steiger
Hagenholzstrasse 56, 8050 Zürich
Tel. 058 311 04 31
simon.steiger@funk-gruppe.ch

CURAVIVA.CH
VERSICHERUNGSDIENST

www.curaviva.ch/versicherungsdienst