Warnung vor falschen Corona -Mails – Erhöhte Cyberrisiken

Weltweit registrieren Unternehmungen einen starken Anstieg von Cybervorfällen. Mit Hilfe von Covid-19 wird die neue Angriffsflut lanciert.

Für Cyberkriminelle ist es typisch, aktuelle Geschehnisse für ihre Betrugs- und Phisingangriffe zu nutzen. In Anbetracht des weltweiten Einflusses von Covid-19 und des hierzu nötigen Informationsbedarfs in der breiten Öffentlichkeit, eignet sich die aktuelle Lage bestens.

Die Wahrscheinlichkeit steigt, dass die Mitarbeiter unsichere Netzwerke nutzen, um von zu Hause zu arbeiten. Die zunehmende Verwirrung und Angst begünstigt zudem, dass Leute schädliche Anhänge auf Grund des Informationsbedarfs anklicken (z.B. gefälschte E-Mails der WHO).

Es ist sehr wichtig, dass verstärkt und auch abteilungsübergreifend Kontrollen und Sensibilisierungen durchgeführt werden:

Empfehlungen für Mitarbeitende

- Links/Anhänge – Klicken Sie keine Links an/öffnen Sie keine Anhänge von unbekannten Absendern. Prüfen Sie E-Mailadressen von Absendern auf deren Richtigkeit.
- Daten/Kennwörter – Geben Sie keine Personenbezogenen Daten/Kennwörter bekannt. Vertrauenswürdige Geschäftspartner verfügen in der Regel bereits über diese Daten resp. benötigen diese nicht.
- Melden – Alle verdächtigen E-Mails sollten dem IT-Verantwortlichen zur Prüfung gemeldet werden.
- Benachrichtigen – Sollte doch etwas Merkwürdiges geöffnet/angeklickt werden, ist der IT-Verantwortliche zu informieren.

SRB Assekuranz Broker AG | Luggwegstrasse 9 | CH-8048 Zürich
T + 41 44 497 87 87 | info@srb.ch | www.srb.ch

Empfehlungen für Unternehmungen

- Mehrstufenidentifikation – Als zusätzliche Sicherheit sollten VPNs mit einer Mehrstufenidentifikation konfiguriert sein.
- Sichere Verbindungen – Das Firmennetzwerk sollte nur über sichere Zugänge genutzt werden (VPN, verschlüsselte Verbindungsverfahren).
- Zugriff – Gibt es Regionen/Länder, aus denen kein Fernzugriff durch Mitarbeitende erfolgen muss? Setzen Sie die IP-Bereiche dieser Regionen/Länder aktiv auf die «schwarze Liste».
- Cloud – Verschärfen Sie die Sicherheitseinstellungen bei der Verwendung von Cloud-Diensten und überwachen Sie Konfigurationsveränderungen/unbefugte Manipulationen.
- Schulung – Schulen und sensibilisieren Sie Ihre Mitarbeitenden regelmässig.
- Firewall - Firewalls sind richtig zu konfigurieren und deren Protokollierung zu überwachen.

Unser Cyber-Experte Herr Ralph Mannhart, Tel. 044 497 87 01 steht Ihnen für weitere Auskünfte gerne zur Verfügung oder melden Sie sich bei Ihrem Kundenbetreuer.

Freundliche Grüsse

SRB Assekuranz Broker AG