ARBONIA

Information Security Newsletter

Geschätzte Mitarbeitende

Gemäss dem Motto ***THINK BEFORE YOU Click.Post.Type*** wollen wir Sie über aktuelle Gefahren im Umgang mit den Informationstechnologien informieren und Sie auf Ihre Mitverantwortung beim Schutz gegen Cyberkriminelle aufmerksam machen. Denn nur gemeinsam können wir die IT-Sicherheit aufrechterhalten und damit die Geschäftstätigkeit und Wettbewerbsfähigkeit der Arbonia Gruppe vor grossen Schäden bewahren.

Die zunehmende Vernetzung, Digitalisierung und das Internet führen zu einem rasanten Anstieg der Cyber Kriminalität. Die Gefährdungslage hat sich weiter verschärft und ist zudem vielschichtiger geworden. Auch unser direktes Geschäftsumfeld blieb in den letzten Monaten von gravierenden Cyber Vorfällen (z.B. Meier Tobler) nicht verschont. Ein angemessener Informationsschutz kann jedoch nicht nur durch technische Massnahmen erreicht werden, sondern hängt auch stark von Ihrem Verhalten und Umgang mit Daten und Informationssystemen ab. Sie sind als Arbonia-Mitarbeiter ein zentrales Glied der Sicherheitskette und müssen diese Verantwortung aktiv wahrnehmen. Die Förderung einer gemeinsamen Informationssicherheits-Kultur in der Arbonia Gruppe ist uns ein sehr wichtiges Anliegen.

Das häufigste und verbreitetste Angriffswerkzeug ist und bleibt das E-Mail, gefolgt von Social Engineering (Manipulation oder Beeinflussung einer Person) und dem Internet. Aus diesem Grund ist es äusserst wichtig, verdächtige Quellen als solche zu erkennen. Ein falsches Verhalten kann zur gravierenden Beeinträchtigung der Geschäftstätigkeit und zu finanziellen Schäden für die Arbonia Gruppe führen. Trennen Sie bei verdächtigen Ereignissen sofort Ihren Computer vom Netzwerk (Netzwerkkabel ausstecken, WLAN ausschalten) und informieren Sie so schnell wie möglich Ihre IT-Abteilung.

Nachfolgend finden Sie einige allgemeine Tipps für Ihren geschäftlichen wie privaten digitalen Alltag:

- **Seien Sie kritisch und haben Sie kein blindes Vertrauen in E-Mails von scheinbar bekannten Absendern**, denn sie könnten gefälscht sein. Lassen Sie sich dazu auch nicht durch persönliche Anreden oder fehlerfrei geschriebenen Text verleiten!
- Fragen Sie im Zweifelsfall in einem separaten E-Mail oder telefonisch beim Absender nach, ob das E-Mail tatsächlich von ihm verschickt wurde. Benutzen Sie bei solchen Rückfragen nie den "Antworten" Button, sondern die Kontakte aus dem Outlook Adressbuch.
- Antworten Sie nie auf verdächtige E-Mails.
- **Öffnen Sie nie verdächtige Anhänge.** Löschen Sie sie im Zweifelsfall oder lassen Sie sie von Ihrer IT überprüfen.
- **Lassen Sie sich bei zweifelhaften telefonischen Anfragen zu keiner Handlung unter Druck nötigen**. Die Angreifer wollen Sie überrumpeln, Ihre Neugierde wecken oder Sie verängstigen, um Sie dann zu einer unbedachten Aktion zu verleiten. Sprechen Sie solche Fälle sofort bei Ihrem Vorgesetzten an.
- Lassen Sie nie Fernwartungs-Verbindungen auf Ihr persönliches Gerät zu, ausser Sie kennen die Person, welche sich mit Ihrem PC oder Laptop verbindet (z.B. interne IT-Helpdesk-Abteilung).
- **Teilen Sie mit niemandem Ihre persönlichen Zugangsdaten.** Es gibt keinen Grund dafür.
- Halten Sie sich stets vor Augen, welche personenbezogenen und geschäftlichen Daten / Informationen Sie preisgeben. Vermeiden Sie geschäftliche Kommunikation über Social Media (z.B. Facebook, Instagram).
- **Verwenden Sie immer starke Passwörter und ändern Sie diese regelmässig.**
- Verwenden Sie Ihre geschäftliche Mail-Adresse ausschliesslich für geschäftliche Korrespondenz, nicht für private Zwecke wie z.B. Webshops oder Wettbewerbsteilnahmen.
- Speichern Sie keine Geschäftsdaten auf Ihrem privaten Gerät und kopieren Sie keine privaten Daten auf Ihr geschäftliches Gerät.
- Scheuen Sie sich nicht, Ihren Vorgesetzten oder die IT-Abteilung bei einem Vorfall zu informieren und involvieren.

Besten Dank für Ihre Unterstützung!

Freundliche Grüsse

Alexander von Witzleben
CEO

Daniel Wüest
CFO

Patrick Langenegger
CIO