ARBONIA

Newsletter Sicurezza Informatica

Stimati collaboratori,

Secondo il motto ***THINK BEFORE YOU Click.Post.Type***, desideriamo informarvi sui pericoli attuali legati all'uso della tecnologia delle informazioni e richiamare l'attenzione sulla vostra corresponsabilità nella protezione dai criminali informatici. Solo insieme infatti possiamo mantenere la sicurezza informatica e proteggere da seri danni l'attività aziendale e la competitività del Gruppo Arbonia.

L'interconnessione e digitalizzazione crescenti e Internet comportano un aumento enorme dei crimini informatici. Il rischio si è intensificato ed è diventato inoltre più complesso. Anche il nostro contesto aziendale diretto non è stato immune negli ultimi mesi da preoccupanti incidenti informatici (ad es. Meier Tobler). Tuttavia non si può conseguire una ragionevole protezione informatica solo mediante misure tecniche; essa dipende molto infatti anche dal vostro comportamento e da come utilizzate i dati e i sistemi di informazioni. In qualità di collaboratori Arbonia, rappresentate un anello centrale della catena di sicurezza e dovete esercitare questa responsabilità in modo attivo. È molto importante per noi promuovere una cultura comune sulla sicurezza informatica all'interno del Gruppo Arbonia.

Lo strumento di attacco più frequente e più diffuso rimane sempre la posta elettronica, seguita dal Social Engineering (manipolazione o condizionamento di una persona) e da Internet. Per questo motivo è essenziale riconoscere le fonti sospette come tali. Un comportamento sbagliato può pregiudicare seriamente l'attività aziendale e causare danni finanziari al Gruppo Arbonia. In presenza di casi sospetti, scollegate subito il vostro computer dalla rete (staccate il cavo di rete, disinserite la rete WLAN) e informate appena possibile il vostro reparto IT.

Di seguito trovate alcuni suggerimenti generali per la vostra vita digitale quotidiana, sia sul lavoro che nella sfera privata:

- **Mantenete un atteggiamento critico e non mostrate una fiducia cieca nelle mail di mittenti apparentemente conosciuti**, perché potrebbero essere false. Non vi lasciate convincere nemmeno da intestazioni personali o da un testo privo di errori!
- Se avete dei dubbi, chiedete al mittente in una mail separata o al telefono se è effettivamente il mittente di quella mail. Per questo tipo di richieste non utilizzate mai il tasto "Rispondi", ma utilizzate i contatti della rubrica di Outlook.
- Non rispondete mai a mail sospette.
- **Non aprite mai allegati sospetti.** Se avete dei dubbi, cancellateli o fateli controllare dal vostro IT.
- **In caso di richieste telefoniche dubbie, non fatevi mai spingere ad agire sotto pressione**. Chi vi attacca vuole cogliervi di sorpresa, suscitare la vostra curiosità o spaventarvi per farvi compiere un'azione non ponderata. In casi del genere contattate subito il vostro superiore.
- Non collegate mai il vostro dispositivo personale a una manutenzione remota, a meno che non conosciate la persona che si collega al vostro PC o portatile (ad esempio il reparto di help desk IT).
- **Non condividete con nessuno i vostri dati di accesso personali.** Non ce n'è motivo.
- Ricordatevi sempre quali dati / informazioni personali e aziendali divulgate. Evitate comunicazioni aziendali tramite i social media (ad es. Facebook, Instagram).
- **Utilizzate sempre password sicure e cambiatele regolarmente.**
- Utilizzate il vostro indirizzo mail aziendale esclusivamente per la corrispondenza aziendale, non per fini privati come acquisti online o partecipazioni a concorsi a premi.
- Non memorizzate dati aziendali sul vostro dispositivo privato e non copiate dati privati sul vostro dispositivo aziendale.
- Non abbiate paura di informare e coinvolgere il vostro superiore o il reparto IT in caso di eventuali incidenti.

Vi ringraziamo per il vostro supporto!

Cordiali saluti

Alexander von Witzleben	Daniel Wüest	Patrick Langenegger
CEO	CFO	CIO