ARES
preventing leaks

ARE YOU SECURE?

Cyber Awareness

DataBreaches, KryptoViren, CEO-Fraud und Phishing auf mobilen Endgeräten – man möchte meinen sich in einer sicheren Infrastruktur zu bewegen – doch plötzlich steht man im Rampenlicht der Medien.

Unternehmen die Hackern zum Opfer fallen, sind meist nur wenig darauf vorbereitet. „Uns wird das nicht passieren!“ oder „Was wollen die schon finden?“ sind ganz alltägliche Aussagen in unserem Tagesgeschäft! Doch hinter den Aktivitäten der Blackhats (Hacker) stecken kriminelle Geschäftsmodelle, die dadurch Umsätze generieren und erhebliche Schäden verursachen.

Zusätzlich wird es für Hacker auch immer einfacher und schöner, denn man kann sich **VERSICHERN**!

Kann man sich gegen Image- und Reputationsverlust versichern? **NEIN!**

Sogenannte „Cyber Versicherungen“ unterstützen das Geschäftsmodell von Hackern, denn wer sich versichert investiert nicht in eine sichere Infrastruktur und bildet auch seine Mitarbeiter/-innen nicht weiter!

Als Unternehmen oder Geschäftsführer steht man im Fokus und kommuniziert in Krisensituationen oftmals in die falsche Richtung. Dies führt dazu, dass sehr schnell **„digitales Lösegeld“** in Form von Kryptowährungen bezahlt wird, in der Hoffnung die Systeme laufen wieder wie gewohnt.

STOP – tun Sie das unter keinen Umständen! In diesen Situationen ist es immens wichtig, seinen „Partner of Trust“ bereits in Rufbereitschaft zu haben.

In einem KRISENFALL erst in Verhandlungen zu gehen und Verträge zu prüfen, würde unheimlich viel Zeit in Anspruch nehmen, die in diesen Momenten keinesfalls zur Verfügung steht!

Wir stehen Ihnen mit unseren internationalen Top-Experten zur Seite und freuen uns auf Ihre geschätzte Kontaktaufnahme.

<u>Gemeinsam mit Raml & Partner stellen wir Ihnen zur Verfügung:</u>

- **1o Verhaltensregeln im Angriffsfall**
- **kostenloses Erstgespräch zur Informationssicherheit**

Jürgen Weiss, CEO
ARES Cyber Intelligence GmbH
+43.676.3109332

ARES
preventing
leaks

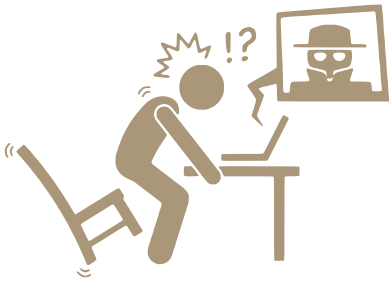
ARE YOU SECURE?

RANSOMWARE

DIE MEIST GEFÜRCHTETE IT- GEFAHR UNSERER ZEIT!

Wenn Deine Infrastruktur skrupellos als Geisel genommen wird, indem eine Schadsoftware diese verschlüsselt. Lösegeld - die Forderung.

„Deine Daten werden verschlüsselt, überweise via Bitcoins zur Wiederherstellung“



Ein Horrorszenario. Eine Meldung die jedem noch so versierten Nutzer den kalten Schweiß auf die Stirn treibt.

Oberste Priorität: Keine Panik!

Wenn ein Backup der verschlüsselten Daten existiert, kann dieses nach der Bereinigung wieder eingespielt werden.

10 Verhaltensregeln im Angriffsfall

1. Call to Action—sofort reagieren!
2. Rechner umgehend vom Netzwerk trennen!
3. Rechner NICHT vom Stromnetz nehmen!
4. WLAN abschalten!
5. KEINE Zahlung tätigen!
6. Dringend Mitarbeiter informieren!
7. ARES Cyber-Experten hinzuziehen!
8. Datenschutzbehördliche Anzeige erstatten!
9. Ursachenforschung & Herkunftsanalyse!
   ARES Expertenaufgabe
10. Aktivierung des letzten Backups!
    ARES Expertenaufgabe

IM KRISENFALL: emergency@ares-ci.com | 0800-0800 22 (gratis Hotline)

ARES Cyber Intelligence GmbH
Security | Digital Transformation | Solutions, Education & Operations (international)