Ein Cybersecurity Briefing für Unternehmer; 5 + 3 Minuten

Als Geschäftsführer und Vorstandsmitglieder wissen Sie genau welches die wertvollen Güter in Ihrem Unternehmen sind und um deren Schutzmassnahmen. Aber wie steht um die Informationssicherheit, Neudeutsch Cybersecurity?

Informationen in jeder Form (Kundendaten, Verträge, Forschungsergebnisse, Prozesse etc.) sind das Lebenselixier für Ihr Unternehmen. Der Schutz von Informationen, deren Verfügbarkeit, Integrität und Geheimhaltung fundamental wichtig für Ihre Geschäftsprozesse ist, entscheidet bei einem Angriff eventuell über den Fortbestand Ihres Unternehmens.

Was sollten Sie über Cybersecurity wissen?

- Cybersecurity betrifft jeden, im privaten Umfeld im geschäftlichen Umfeld
- Es wird nie mehr einen hundertprozentigen Schutz geben. Der Schadenfall ist nur eine Frage der Zeit – das Ausmass können Sie wesentlich beeinflussen!
- Cybersecurity wird meist im Zusammenhang mit Informationsrisiken in digitaler Form benutzt, es ist aber kein reines IT Thema. Menschliche und organisatorische Faktoren spielen eine grosse Rolle
- Nichts tun oder ignorieren ist keine Option, die Bedrohung ist real
- Angreifer mögen es, wenn Sie sich in Sicherheit wiegen, die Security Industrie lebt von der Angst
- Versicherungen decken im besten Fall den direkten finanziellen Schaden ab
- Cybersecurity kann nur erfolgreich sein, wenn sie Sie auf Management Ebene angehen (Top Down). Eine vollumfängliche Delegation in die IT wird langfristig nicht zielführend sein
- Der grösste Gefahrenherd, der Mensch, ist am schwersten zu kontrollieren, d.h. am aufwendigsten
- Zertifizierungen helfen Ihnen nicht im Schadensfall, sie reduzieren Risiken bedingt im Vorfeld
- Effektive Massnahmen müssen nicht zwingend kompliziert und/oder teuer sein

Was sollten Sie tun?

Cybersecurity richtig zu adressieren heisst, eine nachhaltige Informationssicherheitsstrategie in Ihrem Unternehmen zu implementieren; dies adressiert auch nicht digitale Informationen und den Faktor Mensch

- Machen Sie Informationssicherheit zur Chefsache
- Evaluieren Sie Ihren Status Quo, alleine oder mit Hilfe von externen Fachspezialisten
  - Kennen Sie Ihre wichtigsten Informationen und Informationssysteme/Träger?
  - Sind Verfügbarkeit, Integrität und Geheimhaltung definiert?
  - Wie ist die Risikolage für Ihre wichtigsten Informationen und Informationssysteme/Träger?
  - Welche Risikominderungsmassnahmen bestehen?
  - Wie hoch ist das Restrisiko?
- Gliedern Sie Cybersecurity in Ihren Risiko-Management-Prozess ein
- Bauen Sie Fachkompetenz in Ihrem Unternehmen auf

Der 3 Minuten Schnelltest
Wissen Sie wo Ihr Unternehmen steht? Basierend auf obigen Informationen haben wir einen Schnelltest entworfen. Es ist kein wissenschaftlicher Ansatz, mehr ein Test Ihres Bauchgefühls zu diesem Thema.

3 Minuten Investment		Wohlfühlbaro meter	
		☺	😐
1	• Liegt die Verantwortung von Informationssicherheit, Governance-, Risiko- und Compliance-Management (GRC) bei der Unternehmensführung oder ist dieses Thema an das mittlere Management und die Abteilungen delegiert? • Können Sie in 4 Stunden Ihren Status ermitteln? • Sind alle Ihnen bekannten Risiken im Risiko Register registriert?		

2	• Kennen Sie anstehende regulatorische oder Gesetzesänderungen? *Zum Beispiel das neue europäische Datenschutzgesetz welches auch Schweizer Firmen betrifft. Siehe CISS Blog Einträge zu diesem Thema.* • Haben Sie bereits Vorkehrungen zu deren Umsetzung getroffen?		
3	• Kennen Sie Ihre «Kronjuwelen» (Geschäftsprozesse, Systeme, Lieferanten, Personen etc.) und welchen Risiken diese ausgesetzt sind? • Gibt es Gegenmassnahmen für erkannte Gefährdungen?		
4	• Haben Sie Notfallpläne für Ihr Geschäft? *Zum Beispiel nach einem Feuer, einem Virus etc.* • Wenn ja, sind diese aktuell und getestet?		
5	• Wie effektiv und effizient ist Ihr Informationssicherheit, Governance, Risk and Compliance Ansatz in Bezug auf Vermeidung von blinden Flecken, kontinuierlicher Verbesserung, Berichterstattung und Kosten?		
Total			

Wenn Sie insgesamt auf zwei oder weniger ☺ kommen, dann empfehlen wir Ihnen aktiv zu werden.

Unser CISS «ISMS Outline!», ist ein pragmatischer Ansatz für Informationssicherheit/Risiko Management und steht gratis zum Download zur Verfügung unter www.ciss.ch. Viel Spass damit. Anregungen zur Verbesserung sind willkommen. CISS ist spezialisiert auf den «Faktor Mensch» und «organisatorische Informationssicherheit». Mehr Informationen zu diesen Themen finden Sie in unserem Blog.

Andreas von Grebmer – CIS Switzerland