it.sec
security for your information

Und dann kam Corona…

ISMS und Tätigkeit als CISO durch Home Office auf die Probe gestellt

Workshop der GI-FG SECMGT am 11.09.2020 (Webinar)

Vortragender: Bernhard C. Witt
Principal Consultant für Datenschutz und Informationssicherheit

Zum Vortragenden

- **Principal Consultant** für Datenschutz und Informationssicherheit bei der **it.sec GmbH**, Leiter IT Governance, Risk & Compliance Management
- Tätig als Berater, CISO, ISB, DSB und/oder Internal Auditor bei Unternehmen und Behörden bzw. als Prüfer nach § 8a III BSIG
- Industriekaufmann, Diplom-Informatiker
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- zertifizierter ISO/IEC 27001 Lead Auditor (BSi) & CRISC (ISACA)
- Auditor für Recht & Technik DS-erhaltender Verfahren (ADCERT)
- zusätzliche Prüfverfahrenskompetenz nach § 8a III BSIG
- Lehrbeauftragter an der Universität Ulm (seit 2005)
- Autor diverser Bücher zu Datenschutz und Informationssicherheit
- Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit (seit 2009), deren Sprecher seit 11/2016
- Mitglied im Leitungsgremium der GI-Fachgruppe Management von Informationssicherheit (seit 2007), deren Sprecher von 02/2009 – 11/2013
- Mitglied im Leitungsgremium der GI-Fachgruppe Datenschutz-fördernde Technik (seit 2012)
- Mitglied im DIN-Arbeitsausschuss „IT-Sicherheitsverfahren“ AK 1 & 4 (seit 2011)

Zur **it.sec**:
- Seit 1996 tätig
- Penetrationstests
- Datenschutz
- IT GRC Manage-ment
- Teil d. SITS Group

→ www.it-sec.de

Herausforderungen durch Corona (1)

In kurzer Zeit Umstellung auf Home Office

- Ausgabe geschützter **Notebooks**
  - Mussten teilweise erst noch beschafft werden
  - Mussten sicher konfiguriert werden
  - Mussten vorgabengemäß dokumentiert werden
- Ausgabe **2-Faktor-Authentifizierung**
  - Musste generiert und auf Smartphone aufgespielt oder separat ausgegeben werden
- Organisation **Online-Zugang**
  - VPN via WLAN oder Appliance (incl. ausreichend langem LAN-Kabel)
  - Videokonferenz i.d.R. über bestehende IP-Telefonie
  - Anfangs Probleme bei privater Bandbreite

Herausforderungen durch Corona (2)

Abgrenzungsprobleme

- **Home Office vs. Telearbeit**
  - Dauerhaft eingerichteter Fernarbeitsplatz?
  - Ergonomie & Arbeitssicherheit am Fernarbeitsplatz
  - Sichere Dokumentenverwaltung im Home Office
  - Wenn alle zuhause im Home Office sind…
- **Schichtplan** für On-Premise-Arbeiten
  - Aufrechterhaltung der IT-Infrastruktur erfordert teilweise Tätigkeiten vor Ort
  - Arbeitsgruppen disjunkt aufteilen, um auch bei Infektion Einzelner funktionstüchtig zu sein
- **Kurzarbeit vs. Vollstress**
  - Patchen aus der Ferne braucht mehr Zeit
  - Behutsam mit Warnhinweisen umgehen

Herausforderungen durch Corona (3)

Auswirkung auf das ISMS

- Auslösung **Pandemieplan**
  - Krisenstab musste aktiviert werden
  - Sonderregeln für Schlüsselpersonal (inkl. CISO)
    - Begründete Ausnahme für Ausgangssperre
    - Freischaltung Zutrittsbefugnis trotz Lockdown
    - Reiseverbot
- **Not kennt kein Gebot**
  - Aufrechterhaltung der Funktionstüchtigkeit
  - Ziehen Ausnahmeklausel für ISMS-Regeln
  - Nachgelagerte Prüfung Informationssicherheit

Herausforderungen durch Corona (4)

Auswirkung auf die Tätigkeit als CISO (1)

- Keine **„Nebenbei“-Gespräche** mehr
  - Keine Kontaktierung des CISO mehr im Gang, bei Kaffeemaschine oder in der Kantine
  - Kontrollen des CISO nicht mehr „nebenläufig“
  - Nur noch „virtuelle“ Präsenz des CISO
    - Einerseits gesenkte Schwelle für Betroffenenanfragen
    - Andererseits reduzierte Regelkonformität (signifikant mehr Sicherheitsvorfälle aus Fahrlässigkeit)
- Neue Alltagsprobleme kosten **Zeit**
  - Mehr Pausen bei kollaborativem Arbeiten
  - Stärkere Fokussierung auf Einzelthemen
  - Jede Besprechung muss organisiert werden

Herausforderungen durch Corona (5)

Auswirkung auf die Tätigkeit als CISO (2)

- **ISMS** Anpassungen erfolgen nachgelagert
  - Erst die Ausnahme, dann die neue Regel
  - Verantwortung für einzelne Bereiche stärker aufgesplittet
  - Etablierte Regeln stehen auf dem Prüfstand
    - Was hindert, was nützt?
    - Ausführung von Notfallplänen lenkt den Blick auf das Wesentliche
    - Nebensächlichkeiten werden aber plötzlich wichtig
    - Steuerung mittels Kennzahlen wurde unwichtiger
    - Permanente Nachsteuerung nötig („Reparaturbetrieb“)

Lessons learnt

- Ziele sind wichtiger als Maßnahmen
- Erläuternde Handreichungen benötigt für Hilfe zur Selbsthilfe
- Tätigkeit als CISO läuft ausgerechnet an empfindlicher Stelle („Nebenbei“-Gespräche) grundlegend anders ab
  → auf neues „Normal“ einstellen
- Zeit für „Entrümpelung“ des ISMS
- Pausen sind wichtig ;-)

Vielen Dank für Ihre Aufmerksamkeit

it.sec GmbH
Einsteinstr. 55
89077 Ulm

USt-ID Nr.: DE 327012013
Steuernummer: 88002/83062
Amtsgericht Ulm: HRB 739206

vertreten durch den Geschäftsführer **Dipl. Ing. (FH) Holger Heimann.**

Hauptsitz Ulm	Niederlassung Berlin	Niederlassung Wien	Niederlassung St. Pölten
it.sec GmbH	it.sec GmbH	it.sec GmbH	it.sec GmbH
Einsteinstr. 55 **89077 Ulm** **Deutschland**	Borkumstr. 2 13189 Berlin Deutschland	Zweigniederlassung Wien Gußhausstr. 22/4 1040 Wien Österreich	c/o BIZ St. Pölten Büro Top 1.22 Heinrich Schneidmadl-Str. 15 3100 St. Pölten Österreich
Tel: +49 731 20589-0 **Fax: +49 731 20589-29**	Tel: +49 30 2096759-0 Fax: +49 30 2096759-29	Tel: +43 1 3750247-0 Fax: +43 1 3750247-29	Tel: +43 1 3750247-0 Fax: +43 1 3750247-29
info@it-sec.de **www.it-sec.de**	info@it-sec.de www.it-sec.de	info@it-sec.at www.it-sec.at	info@it-sec.at www.it-sec.at