.msg .consulting .solutions .partnership

IT-Sicherheit im Spannungsfeld

München, 01. Februar 2017

Ausgangssituation

Herausforderungen Cybersicherheit aktuell

- Erweiterte staatliche Überwachungsforderungen schaffen Schwachstellen in Systemen, die durch Unberechtigte ausgenutzt werden können
- Sicherheitsvorfälle werden noch immer vertraulich behandelt (verschwiegen). Dadurch tritt kein Lern-Effekt ein
- Forensische Analysen finden zu selten statt. Infektionswege und Angriffstechniken bleiben im Dunkeln.
- End-to-End Encryption und Authentification wird zu wenig eingesetzt (weniger als 30 % aller internet-basierter Mail ist verschlüsselt)
- Awareness und Sensibilisierung halten nicht Schritt mit immer neuen Angeboten am Markt
- Gesetze und Regulierung ist entweder nicht zielgerichtet (zu schwach) oder wirkungslos (unkontrolliert)
- Das Wissens- und Bildungsniveau in Bezug auf Cyber-Bedrohungen ist gering. Hier müsste bereits im Schul-Kontext angesetzt werden.
- Von Security-Spezialisten werden häufig noch veraltete Konzepte und Vorgehensweisen propagiert. Cyber-Security muss sich schneller an veränderte Herausforderungen anpassen

Die Liste erhebt keinen Anspruch auf Vollständigkeit

ZIEL: SICHERER BETRIEB KRITISCHER INFRASTRUKTUREN

Seit Beschluss der Cyber-Sicherheitsstrategie der Bundesregierung im Jahr 2011 werden die Maßnahmen zum Schutz Kritischer Infrastrukturen vor Cyberangriffen konkretisiert.

Gesetzgebung zum Schutz Kritischer Infrastrukturen

Sektorspezifisch

Wesentliche Forderungen und Fristen IT-SiG

In Kraft treten der gesetzlichen Grundlage

- Das IT-Sicherheitsgesetzt ist am 25. Juli 2015 in Kraft getreten
- Der erste Teil der KRITIS-Verordnung zur Umsetzung des IT-Sicherheitsgesetzes ist am 3. Mai 2016 in Kraft getreten

Maßgebliche Forderungen IT-SiG

Betreiber kritischer Infrastrukturen müssen:

- verpflichtend Mindeststandards der IT-Sicherheit umsetzen
- die Wirksamkeit ihrer Umsetzung alle zwei Jahre überprüfen lassen (Audit),
- Meldepflichten erfüllen
- sich vom BSI privilegiert über IT-Vorfälle informieren lassen

Nach in Kraft getretener KRITIS-Verordnung gelten folgende Fristen:

- 6 Monate um die Pflichten zur Meldung erheblicher IT-Sicherheitsvorfälle zu erfüllen
- 2 Jahre, um IT-Sicherheitsstandards nach dem Stand der Technik umzusetzen und dies nachweislich überprüfen zu lassen.

Ordnungswidrigkeiten

Bußgelder wurden erst spät im Gesetz verankert (BSI war hier nicht Treiber)

- Vorkehrungen wurden nicht / nicht richtig / nicht rechtzeitig getroffen
- Keine Kontaktstelle eingerichtet
- Meldungen nicht / unvollständig / nicht rechtzeitig

Geldbußen bis 50.000 €

- Zuwiderhandlung gegen Anordnungen

Geldbußen bis 100.000 €

DIE DATENSCHUTZGRUNDVERORDNUNG

- Veröffentlicht am 4. Mai. 2016.
- Gültig ab dem 25. Mai 2018 verbindlich in allen EU-Staaten
- Löst die Datenschutzrichtlinie 95/46/EG (1995) und das BDSG ab
- Lässt den Ländern Ausgestaltungsspielräume

Ziele:

- Modernisierung des Datenschutzes
- Datenschutz europaweit vereinheitlichen
- Harmonisierung wirtschaftlicher Rahmenbedingungen in der EU

Artikel 25 Absatz 1: Privacy by Desing

Ziele:
Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe
Durchgängige Sicherheit – Schutz während des gesamten Lebenszyklus

Zumutbarkeitsfaktoren:

- „Stand der Technik“
- Implementierungskosten
- Art und Umfang sowie Umstände und Zweck der Datenverarbeitung
- Wahrscheinlichkeit des Eintritts von Risiken
- Schwere der Risiken für die Rechte und Freiheiten der Betroffenen
- Dokumentation des gesamten Prozesses

Artikel 25 Absatz 2: Privacy by Default

Datenschutz als Standardeinstellung
Die Voreinstellungen sind auf Grundlage der Datensparsamkeit zu wählen:

- Menge der erhobenen personenbezogenen Daten
- Umfang ihrer Verarbeitung
- Speicherfrist
- Ihre Zugänglichkeit

Artikel 35: Datenschutzfolgeabschätzung

Ersetzt die bisherige Vorabkontrolle bei

- neuen Technologien die ein „hohes Risiko“ für Betroffenen darstellen.
- automatisierter Verarbeitung (inkl. Profiling) als Grundlage für Entscheidungen
- Umfangreicher Verarbeitung „sensitiver Daten“
- Systematischer Überwachung öffentlich zugänglicher Bereiche
- Datenschutzbeauftragter bestimmt Notwendigkeit einer DSFA

Datenschutzgrundverordnung: Konsequenzen

BDSG

- max. 50k € bzw.
- max. 300k €
- max. 2 Jahre Freiheitsstrafe

DSGVO

- max. 10 Mio. € / 2% Weltjahresumsatz bzw.
- max. 20 Mio. € / 4%
- weitere strafrechtliche Sanktionen durch Staaten möglich

Sanktionsrahmen soll eher ausgeschöpft werden

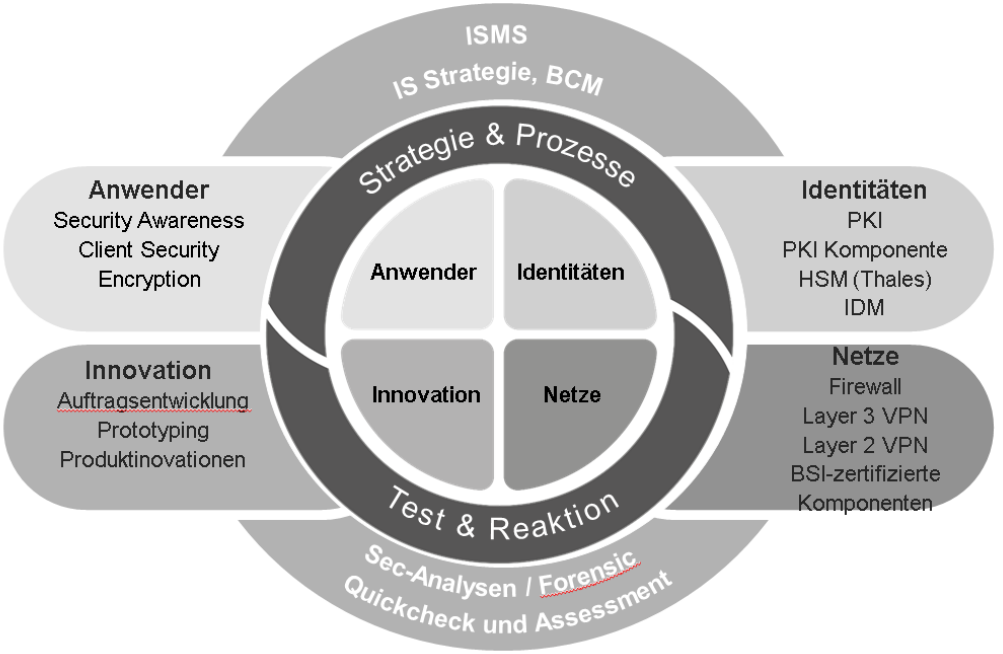
Strafe soll „wirksam, verhältnismäßig und abschreckend“ sein

Ersatzansprüche für immaterielle Schäden möglich: Sammelklage (z.B.: durch Verbraucherverbände)

Geeignete Methodik

- Risikoorientierter Ansatz: Das Risiko bestimmt die Maßnahmen
- IT-Sicherheit und Datenschutz praxisnah und rechtzeitig
- Einstieg in ein ISMS, welches aber bereits „Basis-Schutz“ ermöglicht
- modulares, kosteneffizientes Vorgehen
- Einbeziehung von Vorhandenem (z.B. ITSM)
- „alternative“ Ansätze z.B. ISIS 12, Branchenstandards, Best Practices

Auswahl hochwirksamer und zielführender Maßnahmen



Westphal, Jens
Abteilungsleiter Security Solutions

+49 (0) 175 / 5703757
Jens.Westphal@msg-systems.com

msg systems ag
Robert-Buerkle-Str. 1, 85737 Ismaning
Germany

www.msg-systems.com

.msg .consulting .solutions .partnership