Informationstag "IT-Sicherheit in der Marktforschung"

Gemeinsame Veranstaltung von

Bundesverband IT-Sicherheit e.V.

Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.

Deutsche Gesellschaft für Online Forschung e.V.

Verband der Marktforscher Österreichs

10.06.2016

Wirtschaftskammer Wien, Blauer Saal, Schwarzenbergplatz 14, 1010 Wien

ENTWICKLUNG DER INFORMATIONSSICHERHEIT IN DEN MARKTFORSCHUNGSINSTITUTEN

Harald Neustetter, BSc

10.06.2016

Eckdaten zu meiner Person

- Harald Neustetter, BSc
- Wirtschaftsinformatiker
- 23 Jahre in der IT Branche
- GfK Austria seit 2002
  - 2010 IT Manager
  - 2015 Datenschutzbeauftragter
- Kontakt
  - E-Mail: harald.neustetter@gfk.com
  - XING
  - in

Was umfasst Informationssicherheit

Informationssicherheit 1/2

- Informationen werden verarbeitet
  - in Rechnersystemen
  - auf Papier
  - in den Köpfen der Nutzer
- Schutzziele sind
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität
  - …

Informationssicherheit 2/2

- Gefährdung durch
  - Vorsätzliche Handlungen
  - Höhere Gewalt
  - Organisatorische Mängel
  - Menschliche Fehlhandlungen
  - Technisches Versagen
- Umsetzung eines angemessenen Sicherheitsniveaus
  - Schutz vor Gefährdung von außen und innen
  - Vermeidung von Straftaten durch Mitarbeiter oder Hacker
  - Schutz personenbezogener Daten
  - Erfüllung weiterer Verpflichtungen: TKG, DSG 2000, ..
  - Erfüllung vertraglicher Verpflichtungen

Sicherer Umgang mit Informationen

- Wettbewerbsentscheidend
- Schutz finanzieller Interessen
  - Kunde erwartet korrekte und vertrauliche Abwicklung
  - Unternehmen hat Anspruch auf Schutz von Vermögen und Eigentum
- Persönlichkeitsschutz
  - Recht jeder Person über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu entscheiden
- Schutz vor Imageverlust
  - Verlorenes Vertrauen der Kunden
  - Ruf des Unternehmens
- Rechtliche Konsequenzen

Aus vergangenen Tagen …

Erinnern Sie sich noch?

- 1982: ein 15 jähriger und „sein“ Gedicht
  - „Elk Cloner“
  - erster Virus in „freier“ Wildbahn
  - verbreitete sich über Disketten
  - befallene Rechner blieben aber unversehrt
- Durch Internetzeitalter
  - sorgloser Umgang mit neuem, unsicheren Medium
  - schnellere Verbreitung von Viren, Würmern und Trojanern
  - Nimda, SQL / Slammer, Loveletter, Blaster, Sasser, ….
  - „Technisierung“ von Geschäftsprozessen erhöhen das Ausfallsrisiko
- Folgen
  - Schadenspotential wuchs
  - damit auch die Kosten für Beseitigung
  - Kosten für Prävention

Aktuelle Herausforderungen

Der Server eines Softwaredienstleisters, der Apotheken betreut, war Ziel von Angriffen. Vermutlich sind 2000 Patienten betroffen.

25.09.2013 | 17:44 | (Die Presse)

Wien. Digital gespeicherte Daten landen durch einfaches Kopieren irgendwann einmal dort, wo sie eigentlich nicht hingehören. Es ist nur eine Frage der Zeit, bis die falsche Person den richtigen Mausklick macht.

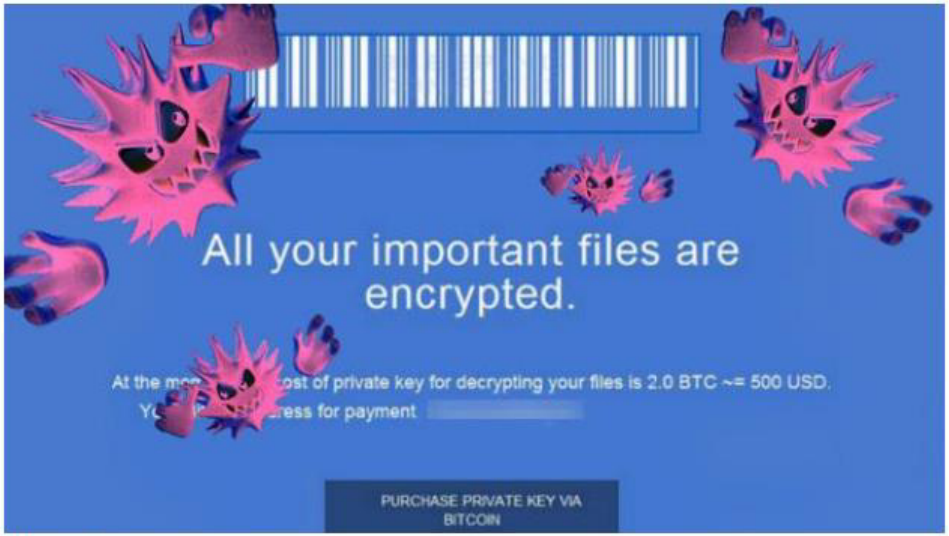
Dass an dieser These etwas dran ist, scheint sich derzeit wieder zu bestätigen. Dem Österreichischen Apothekerverlag dürften in den vergangenen Jahren nämlich unzählige Datensätze von Patienten gestohlen worden sein. Über das tatsächliche Ausmaß des Verlusts kann derzeit aber nur spekuliert werden.

Dabei wäre der Abfluss der Patientendaten beinahe unbemerkt geblieben. Verhindert hat das eine Computerfestplatte, die ein Anonymus einem Journalisten des Magazins „News“ übergeben hat. Die Zeitschrift sichtete das Material und konfrontierte schließlich den Apothekerverlag mit dem Inhalt der Festplatte. „Bis zu diesem Zeitpunkt hatten wir keine Ahnung davon, dass irgendwer Daten von uns gestohlen haben könnte“, sagt Martin Traxler, Geschäftsführer des Apothekerverlags, zur „Presse“.

Quelle: http://diepresse.com/home/panorama/wien/1457171/Patientendaten-gestohlen_Hacker-ubernahmen-Server

Ransomware-Virus legt Krankenhaus lahm

heise online 12.02.2016 12:48 Uhr – Detlef Borchers vorlesen



(Bild: heise Security)

Ein Computervirus hat die IT des Lukaskrankenhauses in Neuss infiziert. Patientendaten sollen dank Backup in Sicherheit sein. Zwei weitere Kliniken sollen auch befallen sein.

Ein als Anhang einer E-Mail verschickter Virus hat sich als hartnäckig resistenter IT-Schädling im Neusser Lukaskrankenhaus eingeschlichen. Das Krankenhaus ist derzeit nur eingeschränkt funktionsfähig, weil viele

Update:

US-Krankenhaus zahlt 40 Bitcoins Lösegeld

Quelle: http://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html

FAKTEN

Donnerstag, 28. Januar 2016 von Rainer Fleckl

FACC: Betrug mit Fake-President-Trick

Wie der Luftfahrt-Zulieferer um 50 Millionen Euro erleichtert wurde

© Bild: APA/Daniel Scharinger

JETZT LESEN

FAKTEN

BP-Wahl: Schieder kritisiert "viele Schlampereifehler"

SPÖ-Klubchef: Zwar keine Auswirkungen auf Wahlausgang, aber auf Stimmung

Die Mail kam von ganz oben, vom Vorstandschef persönlich. Unter dem Siegel der strengsten Verschwiegenheit wurde eine Mitarbeiterin des österreichischen Luftfahrtzulieferers FACC während der Weihnachtstage angewiesen, 50 Millionen zu überweisen. Das Geld, so stand es in der Nachricht, sollte für eine geheime Firmenübernahme im Ausland verwendet werden. Also: geheime Kommandosache, kein Wort zu niemandem.

Die Mitarbeiterin tat, wie ihr geheißen. Und transferierte die 50 Millionen Euro offensichtlich auf Konten im Ausland.

Tatsächlich stammte die Mail an die FACC-Angestellte nicht vom Vorstandsvorsitzenden Walter Stephan, sondern von Internet-Betrügern, die sich des Fake-President-Tricks bedienten. Dabei wird versucht,

Quelle: http://www.news.at/a/facc-betrug-fake-president-trick-millionen

Massive DDOS-Attacke: A1 wurde Opfer von Erpressern

A1 (Telekom Austria) wurde am 1. Februar das Opfer massiver DDOS-Attacken. Mit dem massenhaften Versenden von Datenpaketen aus mehreren Herkunftsländern sollte das System lahmgelegt werden, teilte A1 heute mit.

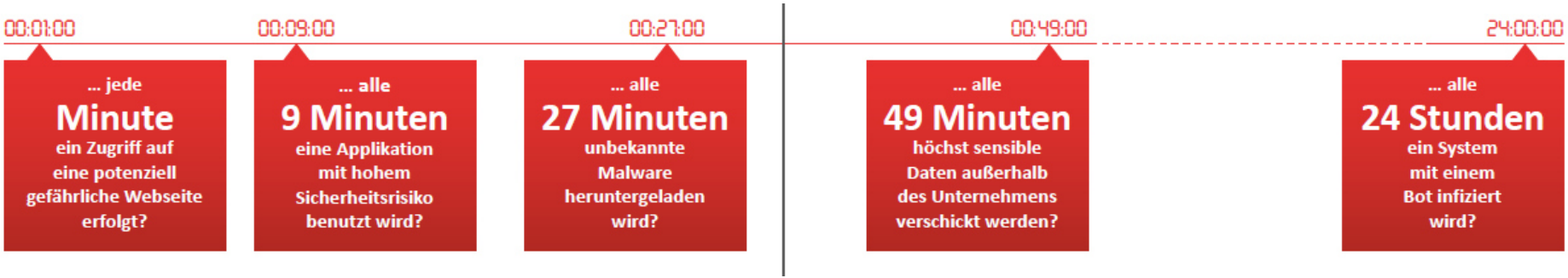
Das Motiv der Cyberattacken war laut A1 Geld: In einem Erpresserschreiben wurden zunächst 100.000 Euro in Bitcoins verlangt, die Forderungen wurden in den folgenden Stunden um das Mehrfache erhöht. Erst als die Erpresser erkannten, dass die Techniker imstande waren, den Angriff abzuwehren, gaben sie laut Angaben ihr Unterfangen auf.

Angriffe aus mehreren Ländern

Das Datum des Angriffs war laut Telekom-Austria-Technikvorstand Marcus Grausam nicht zufällig gewählt: Es war der erste Tag der Semesterferien, sodass die Täter davon ausgehen konnten, dass ein Teil der Techniker auf dem Weg in den Urlaub und damit nicht verfügbar war.

Quelle: http://orf.at/stories/2327821/

Hätten Sie das gedacht?



Quelle: www.bacher.at/checkup

Aktuelle Herausforderungen 1/4

- 3 Cyber-Risiken laut World Economic Forum
  - Cyber-Attacken
  - Datenbetrug und –diebstahl
  - Fehler bei kritischer Infrastruktur

Quelle: http://www3.weforum.org

- Information als Wirtschaftsfaktor auch für Kriminelle
  - Verkauf der Daten über Darkweb
  - ~ 1,8 Mrd. Benutzerdaten im LeakedSource
  - zu LinkedIn und Facebook kommen nochmals
  - 32 Mio. Nutzerdaten aus Twitter

http://www.computerbild.de/artikel/cb-News-Internet-Twitter-Mehr-als-32-Millionen-Konten-gehackt-15742357.html

Aktuelle Herausforderungen 2/4

- Cyber-Straftaten
  - 2016 ist das Jahr der Erpressungen
  - Crypto-Ransomware
  - Datendiebstahl und -verkauf
  - Schädliche Online-Werbung (Malvertising-Angriffen)
- DDoS Attacken
  - Überlastung der notwendigen Bandbreiten
  - Überlastung der Zustandstabellen
  - Überlastung auf Applikationsebene
- Spam & Spionage
  - Social Engineering
  - Phishing/Spear Phishing
  - Vishing (Voice Phishing)
  - Shoulder Surfing / Dumpster Diving

Aktuelle Herausforderungen 3/4

- Mobile Endgeräte - Mobile Marktforschung
  - Mobile Schädlinge nehmen zu – Endpoint Security!
  - Guidelines und Policies definieren
  - Privacy Filter benutzen
  - Daten sammeln und sicher übertragen
  - Verlust/Diebstahl
- Daten und Dokumente schützen
  - Klassifizieren
  - Passwortschutz verwenden
  - Auch PDF‘s sichern
  - Festplattenverschlüsselung
  - Clear Desk Policy
- Datenübermittlung
  - Verschlüsselung bei E-Mails, FTP und Web Zugängen/Portalen
  - Vorsicht mit USB Sticks

Aktuelle Herausforderungen 4/4

- Cloud Dienste
  - Welche Daten und Dienste auslagern?
  - Wo liegen meine Daten? EU? USA? ..
  - Zertifizierte Cloud Dienste verwenden (ISO/IEC 27018)
  - Kunden informieren und Verträge darauf auslegen
  - Verfügbarkeitsgarantie?
  - Rechtliche Aspekte und Haftungsfragen
- Schaffen von Awareness bei den Mitarbeitern
  - Regelmäßige Schulungen
  - Security Awareness Trainingsprogramme durchführen
  - IT Richtlinien und Policies definieren und kommunizieren
- Umgang mit Sozialen Netzwerken und Medien
  - Gute Datenquelle für Sekundärforschung
  - Wer kommuniziert welche Inhalte?
  - Richtlinien definieren

Zukünftige Herausforderungen

Zukünftige Herausforderungen 1/2

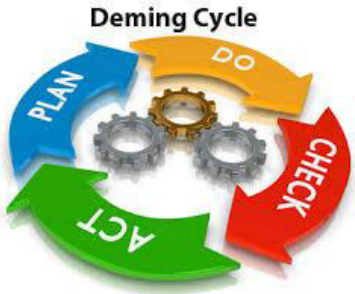
- Digitale Transformation
  - Big Data – Wo liegen diese Daten gerade?
  - Wem gehören die Daten?
  - Suchmaschinenrecherche für Sekundärforschung
  - IoT (Internet of Things)
- Maßnahmen gegen Angriffen/Erpressungen
  - Systeme härten, Patchmanagement, aktuelle Hardware und Software einsetzen
  - IDS/IPS (Intrusion Detection/Prevention System)
  - Scrubbing Center gegen DDoS Attacken
  - Checklisten, Notfallspläne erstellen und regelmäßig **testen**!!!
  - Verstärktes Überwachen von Zugängen, Logfiles, Datenzugriffen, …
- Zertifizierungen für ISMS, ITSM, Datacenter Zertifizierung EN 50600, …
  - Schafft vertrauen beim Kunden (möglicher Wettbewerbsvorteil)
  - Erleichtert Audits

Zukünftige Herausforderungen 2/2

- 2016/679 EU-Datenschutz-Grundverordnung (EU-DSGVO)
  - Beschlossen am 14.04.2016 durch EU Parlament
  - Inkrafttreten ab 25.5.2016
  - Anwendbar ab 25.5.2018
  - Einarbeiten nationaler „Interessen“ noch möglich
  - Besteht aus 99 Artikel und 173 Erwäggründe
  - Ersetzt 95/46/EG Datenschutzrichtlinie -> DSG 2000 (D: BDSG)
- Safe Harbor -> Privacy Shield
  - Seit Oktober 2015 für ungültig erklärt
  - Privacy Shield als Nachfolger soll 2016 aktiv werden
  - Für Zwischenzeit -> Übergangsverträge

Ein Gedanke noch im Umgang mit Informationssicherheit…

- Stop
  - Nicht unüberlegt und
  - unstrukturiert handeln
- Think
  - Passt die Informationssicherheit noch?
  - Muss etwas geändert werden?
  - Und wenn ja, was und wie?
- Act
  - Strategisch und ganzheitlich vorgehen
  - Regelmäßig Überprüfung der Informationssicherheit
  - Deming Cycle (PDCA)



DANKE FÜR IHRE AUFMERKSAMKEIT