Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Information Security Management
01 Intro & Repetition

HSLU – Informatik

Mathias Bücherl (M.Sc.)

Tel. +41 79 746 10 98

mathias.buecherl@hslu.ch

Mit Material von Prof. Dr. Peter E. Fischer, Prof. Armand Portmann und Oliver Hirschi

Agenda

1. Administratives, Einführung
2. Motivation
3. Repetition als Übung: kleine Präsentationen
4. Diskussion und Ergänzungen
5. Nachbearbeitung
6. Vorbereitung auf nächste Woche

Information Security Management

- Was verstehen Sie darunter?
- Warum haben Sie sich für dieses Modul entschieden?
- Was erwarten Sie von diesem Kurs?
- Welche Themen interessieren Sie besonders?
- _____
- _____
- _____
- _____
- _____
- _____

Agenda

1. Administratives, Einführung
2. Motivation
3. Repetition als Übung: kleine Präsentationen
4. Diskussion und Ergänzungen
5. Nachbearbeitung
6. Vorbereitung auf nächste Woche

Daten, Information und Wissen

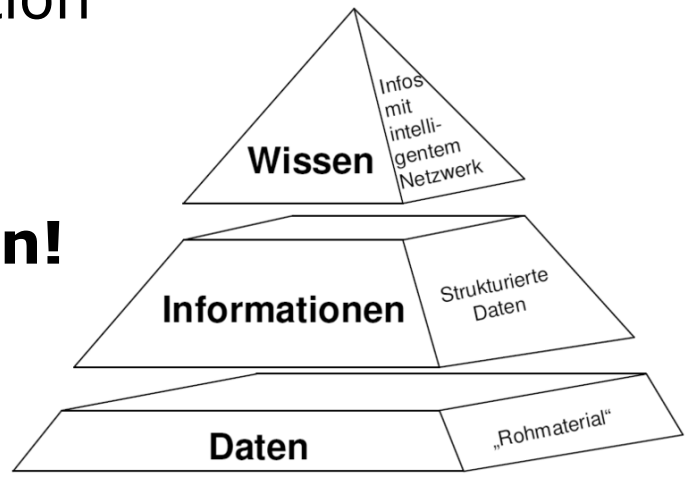
„Information ist die Verknüpfung von Daten in Form von Zahlen, Worten und Fakten zu interpretierbaren Zusammenhängen. Durch die Vernetzung von Informationen entsteht Wissen, das zunächst personenbezogen ist.“

Informationssicherheitshandbuch für die Praxis

Information – Die Grundlage der Informationsgesellschaft

- Wissen ist Macht [Francis Bacon, 1561-1621]
- Wissen ist zur entscheidenden Produktivkraft moderner Ökonomien geworden. Es ist der Rohstoff des 21. Jahrhunderts. [Ralf Fücks]
- „Wissen“ als vernetzte Information

- **Informationen müssen vor Missbrauch geschützt werden!**



wikipedia.org

Was gefährdet die Informationen?
Welche Gefährdungen/Bedrohungen gibt es?

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

Täter

- Frustrierte Mitarbeitende
- Geheimdienste (Echelon, Onyx, …)
- Industriespionage
- Hacker/Cracker
- Whistleblower
- Softwareentwickler (Back Doors)
- Fremdpersonal (externe MAs)
- Administratoren

07.03.2011 Drucken | Senden | Feedback | Merken

Frankreich

Hacker attackierten Finanzministerium

Corbis

Computer-Krimineller: Hacker tragen Brillen, dachte sich dieser Illustrator

150 Rechner sollen betroffen gewesen sein: Das französische Finanzministerium ist zum Ziel eines Hackerangriffs geworden. Offenbar waren die Angreifer an Unterlagen über die G-20-Verhandlungen interessiert.

Paris - Frankreichs Haushaltsminister François Baroin bestätigte die Angriffe gegenüber einem französischen Radiosender. "Das Militär kümmert sich jetzt darum", sagte Baroin am Montag. Es gebe bereits eine Spur, die aber zu bestätigen derzeit "unmöglich" sei.

Das Magazin " Paris Match" berichtet, dass mehr als 150 Rechner von Spionagesoftware

Vorsätzliche Manipulation

- Angriffe über das Internet
- Unerlaubter Zugriff auf Systeme
- Abhören und Modifizieren von Daten
- Angriff auf die Verfügbarkeit von Systemen
- Missbrauch von Systemen, Distributed Denial of Service (DDOS)
- Viren, Würmer und Trojanische Pferde
- Drive by Infection

Blick.ch e-Paper Leserreporter Shop Login

Home News Sport People Unterhaltung

Schweiz Regional Ausland Politik Wirtschaft Wetter

Blick.ch » News » Schweiz » Hacker attackieren Postfinance

Vergeltung für Wikileaks

Hacker attackieren Postfinance

BERN - Postfinance.ch ist die ganze Nacht nicht erreichbar. Dahinter stecken Hacker, die wegen Wikileaks zur «Vergeltung» aufgerufen haben.

Aktualisiert um 09:48 | 07.12.2010

Wikileaks-Chef Julian Assange betrieb ein Konto zur Finanzierung seiner Organisation bei der Postfinance. Über dieses Konto flossen die Spenden-Gelder. Doch Postfinance beendete die Geschäftsbeziehungen mit Assange – weil er als Wohnort fälschlicherweise Genf angegeben hatte.

Im Internet sorgte dies für Aufregung. Hacker, die sich «Anon_Operation» nennen, riefen per Twitter zu der «Operation Payback» («Operation Vergeltung») auf und konzertierten eine DDoS-Attacke auf die Server von Postfinance.ch. Dabei starten tausende infizierte Computer gleichzeitige Anfragen an den Server, was diesen lahmlegen soll.

Mit Erfolg. Postfinance.ch ist nur noch schwer oder gar nicht mehr erreichbar. «Unsere Server sind massiv überlastet», so Sprecher Marc Andrey zu Blick.ch heute

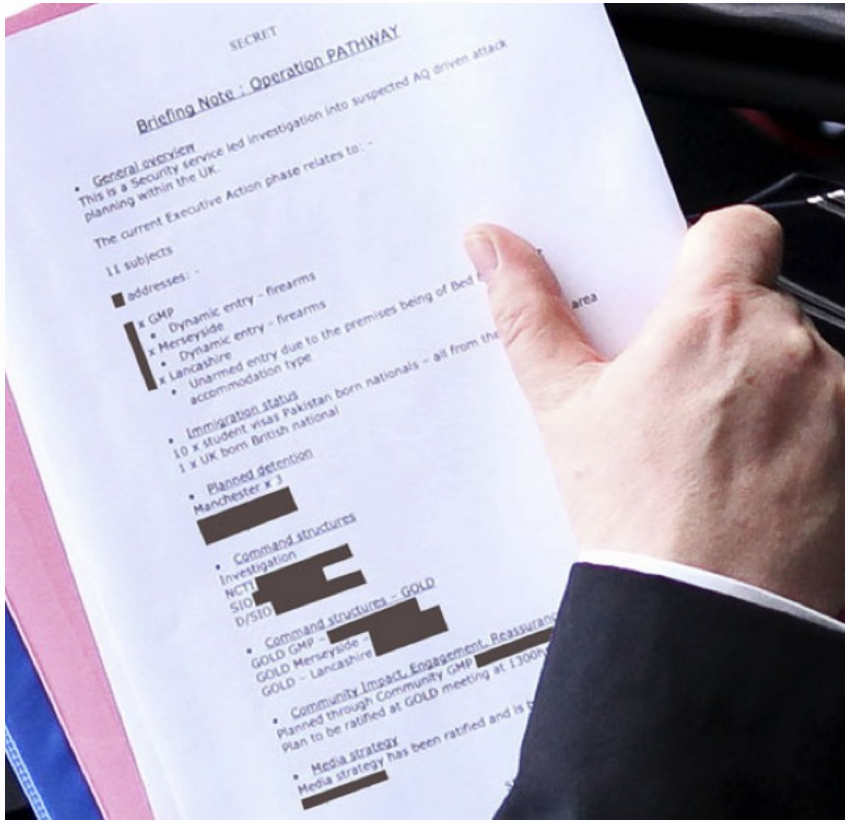
Operation: Payb

So präsentieren sich die Hacker auf dem Twitter-Account. (ZVG)

Menschliches Fehlverhalten

- Fahrlässigkeit
- Gleichgültigkeit
- Unwissenheit
- Leichtgläubigkeit

Bob Quick, ex Scotland Yard



Organisatorische Schwachstellen

- Fehlendes Sicherheits-verständnis des Managements
- Unklare Verantwortlichkeiten
- Ungenaue oder fehlende Abläufe / Prozesse
- Mangelhafte Richtlinien
- Fehlende Strategie und Konzepte
- Mangelhafte Awareness der Mitarbeitenden
- Fehlende Kontrollen

Datenschutzbeauftragter INFO
Informationen zum Datenschutz

Herzlich Willkommen!
Dieser Datenschutz-Blog
Datenschutzbeauftragten

Datenleck bei Werder Bremen

Donnerstag, 8. Juli 2010, 9:13 Uhr

Kategorie: Datenschutz, News, Skandal — kein Kommentar

Am 28. Juni hat es den **Bundesligisten Werder Bremen** erwischt: Etwa zwei Stunden lang konnten Daten von knapp 35.000 Mitgliedern eingesehen werden. Darunter nicht nur **Daten wie Name und Adresse, sondern auch Geburts- und Kontodaten**.

Laut Weser-kurier.de

> „war am Montag im Newsletter ein Link auf eine Fotodatei eingebunden, die das (noch größtenteils verdeckte) neue Werder-Trikot zeigte. Über den Link konnte man aber nicht nur die Fotodatei öffnen, sondern **aufgrund einer fehlenden Sicherung auch auf den Server des Dienstleisters von Werder Bremen** gelangen."

Doch ganz so harmlos wie der Verein den Vorfall darstellen möchte, ist er tatsächlich nicht: **Immerhin gab es 14 Kontakte auf den Server**, die Werder allerdings als eher zufällig abtat. **Doch die Kenntnis von fremden Kontoverbindungen ermöglicht den Zugriff auf das jeweilige Konto** – etwa per Lastschrift. Die betroffenen Mitglieder sind also gut damit beraten, ihre **Kontostände regelmäßig zu überprüfen**.

Erst fünf Tage nach dem Vorfall habe der Verein beschlossen, **die Mitglieder über den Vorfall zu unterrichten**. Und dass, obwohl es mittlerweile nach **§ 42 a BDSG eine besondere Informationspflicht** gibt, wonach sowohl die Aufsichtsbehörde als auch der Betroffene über einen derartigen Vorfall zu unterrichten ist. Dem Gesetzeswortlaut nach

Technisches Versagen

- Ungenügende Wartung
- Nicht funktionierende Überwachungssysteme (z.B. IDS etc.)
- Falsch dimensionierte Systeme
- Fehlerhafte Konfiguration
- Fehlerhafte Applikationen / Betriebssysteme / Firmware / Treiber

Höhere Gewalt

- Unwetter, Erdbeben, Überschwemmungen, Vulkanausbrüche
- Feuer, Wasser
- Ausschreitungen, Geiselnahme, Krieg

Hochwasser Australien 2010

Verantwortung

- Fehlende Informationssicherheit kann den Geschäftsfortgang stören oder verunmöglichen
- Der Schutz der Informationen gehört zur Sorgfaltspflicht des Managements
- Verantwortung kann nicht delegiert werden!

  „Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.“
  (OR Art. 754 Absatz 2)

Die Überwachung der Informationssicherheit ist Chefsache!

Ohne Management-Support geht gar nichts!

- Keine Ressourcen (Zeit und Geld)
- Keine Kompetenzen (Befehls- und Umsetzungsgewalt)
- Keine Priorität

Das Management trägt die Risiken und entscheidet über die eingesetzten Ressourcen!

Oft gehörte Sicht des Managements

- Was bringt uns Informationssicherheit?
  …ausser Kosten?
- Wir haben ja schon eine Firewall, …oder wie das Ding auch immer heisst?
- Unser Unternehmen ist kein lohnendes Ziel für Hacker!
- Bei uns ist noch nie etwas passiert!
- Unsere Mitarbeiter sind 100% loyal!
- Wir können auf unsere Computer problemlos einige Tage verzichten!

Was passiert, wenn wir nichts machen?

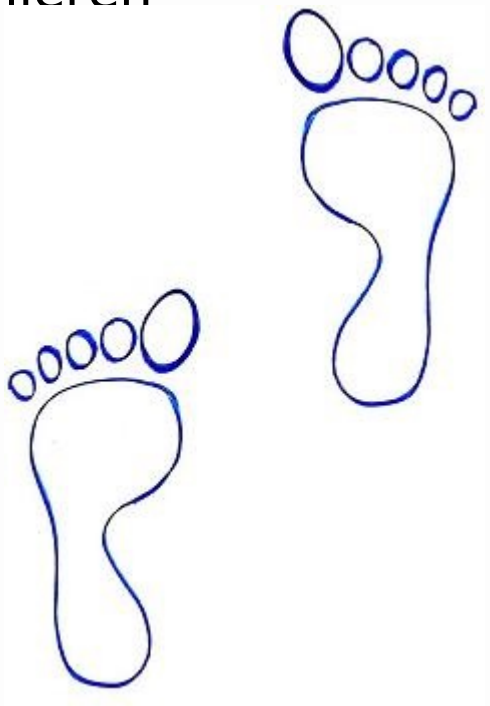
- Kompletter Datenverlust führt in über 50% der Fälle zum Konkurs innert 24 Monaten
- Die Beschaffung und der Aufbau eines Standard-Ersatzsystems dauert mindestens 36h (falls kein Ersatzsystem direkt vor Ort verfügbar)
- Datendiebstahl (wird in den wenigsten Fällen bemerkt)
- Kommen vertrauliche Daten an die Öffentlichkeit, ist der Image-Verlust bei den Kunden je nach Unternehmen immens
- Verletzung gesetzlicher Vorgaben kann strafrechtliche Folgen haben
- Verletzung der Sorgfaltspflicht

Nutzen der Informationssicherheit

- Geringere Verwundbarkeit
- Keine falsche Sicherheit
- Bewussterer Umgang mit Informationen
- Gefahren kennen
- Bewusstes Eingehen von Risiken / Restrisiko bekannt
- Sorgfaltspflichten erfüllt

Wie anpacken?

- Management ins Boot holen
- Prozess der Informationssicherheit etablieren
- Verantwortlichkeiten festlegen
- Sicherheit allumfassend betrachten
- Schrittweise und stetig umsetzen



Agenda

1. Administratives, Einführung
2. Motivation
3. Repetition als Übung: kleine Präsentationen
4. Diskussion und Ergänzungen
5. Nachbearbeitung
6. Vorbereitung auf nächste Woche

Übung Repetition 1

- Gruppieren Sie sich zu viert
- Erarbeiten Sie unter Zeitdruck (wie im richtigen Leben)
- Präsentieren Sie (pptx oder saubere Charts) die Ergebnisse

1. Gruppe: Grundbegriffe
   - Schutzziele (ausführlich), Sicherheit, Risiko (E, S)
   - Unterschied InfoSec – IT-Sec – Integrale Sec
   - Unterschied Identität – Authentizität – Authentifizierung
   - 3 Säulen der InfoSec
   - Unterschied Zutritt, Zugang, Zugriff

Übung Repetition 2

- Gruppieren Sie sich zu viert
- Erarbeiten Sie unter Zeitdruck (wie im richtigen Leben)
- Präsentieren Sie (pptx oder saubere Charts) die Ergebnisse

2. Gruppe: Standards und Frameworks
   - ISO 2700x, x=1-5
   - BSI 200-x, x=1-4
   - BSI Grundschutzkataloge
   - NIST Framework
   - ICT Minimal-Standard

Übung Repetition 3

- Gruppieren Sie sich zu viert
- Erarbeiten Sie unter Zeitdruck (wie im richtigen Leben)
- Präsentieren Sie (pptx oder saubere Charts) die Ergebnisse

3. Gruppe: ISMS und Prozesse
   - Was ist ein ISMS (ausführlich)?
   - Welche Prozessmodelle nutzt man in InfoSec?
   - Wie werden diese genutzt (Bezug zu Standards)?

Übung Repetition 4

- Gruppieren Sie sich zu viert
- Erarbeiten Sie unter Zeitdruck (wie im richtigen Leben)
- Präsentieren Sie (pptx oder saubere Charts) die Ergebnisse

4. Gruppe: Risiko-Management
   - Zugrunde liegende Standards
   - IT-Grundschutz
   - Prozess der Risiko-Analyse (des –Managements)
   - Kombinierte Risiko-Analyse

Übung Repetition 5

- Gruppieren Sie sich zu viert
- Erarbeiten Sie unter Zeitdruck (wie im richtigen Leben)
- Präsentieren Sie (pptx oder saubere Charts) die Ergebnisse

5. Gruppe: Policies
   - Welche Arten von Policies / Konzepte / Richtlinien?
   - Warum benötigt man so viele unterschiedliche?
   - Abhängigkeiten von übergeordneten Dokumenten

Übung Repetition 6

- Gruppieren Sie sich zu viert
- Erarbeiten Sie unter Zeitdruck (wie im richtigen Leben)
- Präsentieren Sie (pptx oder saubere Charts) die Ergebnisse

6. Gruppe: Awareness
   - Berichten Sie über Motivation, Notwendigkeit
   - Wichtige Grundsätze zum Erfolg (KPI)
   - 3 Beispiele für Awareness-Kampagnen

Agenda

1. Administratives, Einführung
2. Motivation
3. Repetition als Übung: kleine Präsentationen
4. Diskussion und Ergänzungen
5. Nachbearbeitung
6. Vorbereitung auf nächste Woche

Ergänzungen

Hier eintragen!

-
-
-
-
-
-
-
-
-

Agenda

1. Administratives, Einführung
2. Motivation
3. Repetition als Übung: kleine Präsentationen
4. Diskussion und Ergänzungen
5. Nachbearbeitung
6. Vorbereitung auf nächste Woche

Nachbearbeitung

- Beantworten Sie die Kontrollfragen (Ilias)
- Gehen Sie alle Präsentationen nochmal durch:
  - Die Einführung (diese Datei)
  - Alle Ergebnis-Präsentationen der heutigen Übung
  - Die relevanten Präsentationen aus ISF

Agenda

1. Administratives, Einführung
2. Motivation
3. Repetition als Übung: kleine Präsentationen
4. Diskussion und Ergänzungen
5. Nachbearbeitung
6. Vorbereitungsauftrag

Termpaper-Themen und Einteilung

- Evtl. noch Klärung der Zuteilung