T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2014
Berlin, 03. - 04.11.2014

IT-Sicherheit bei einem Wikileaks-Partner:
Awareness-Kampagne im Norddeutschen Rundfunk

Karl-Jürgen Hanßmann
Norddeutscher Rundfunk, IT-Sicherheitsbeauftragter

Agenda

1. Warum man „Awareness“ nicht verwenden sollte.
2. Motivation und Anlass der Kampagne im NDR
3. Zielgruppen, Leitgedanken, Lernziele und Inhalte
4. Verwendete Medien
5. Zielerreichung
6. Nachhaltigkeit
7. Umgang mit den Auswirkungen der Snowden-Veröffentlichungen

Warum man „Awareness“ nicht verwenden sollte.

- **„Awareness“ ungefähr = Aufmerksamkeit, Bewusstsein , Bewusstheit, Erkenntnis (leo.org)**
- **Keine exakte deutsche Übersetzung vorhanden**
- **=> Prägnanter Anglizismus, kein “Denglish“**
- **Hat aber leider IT-Sicherheits-Jargon bisher nicht verlassen - noch keine allgemeine Verbreitung in Deutschland**
- **=> Begriff fand keine Akzeptanz im NDR**
- **Daher wurde es eine „Informationskampagne zur IT-Sicherheit im NDR“**

Motivation und Anlass der Informationskampagne

- **NDR erkennt 2010 / 2011 starken Anstieg der IT-Sicherheitsrisiken**
- **Notwendigkeit unternehmensübergreifender und arbeitsrechtlich verbindlicher Regelungen**
- **Dienstanweisung IT-Sicherheit durch Intendanten (seit 1.1.2012 in Kraft)**
- **Definition der Verantwortlichkeiten: Rolle der Informationsverantwortlichen definiert**
- **Ausarbeitung IT-Sicherheitskonzept durch eine Koordinationsgruppe mit Vertretern aus allen Bereichen des NDR (u.a. Benutzerleitfaden zur IT-Sicherheit)**

Zielgruppen

- **Direktorinnen und Direktoren**
- **Mittlere Führungsebene**
- **Obligatorisch für alle Mitarbeiter(innen) in IT-Bereichen**
- **Alle Mitarbeiter(innen) in Produktion und Verwaltung**
- **Alle Mitarbeiter(innen) in den Redaktionsbereichen**
- **Freie Mitarbeiter(innen)**

Leitgedanken

- **Über Risiken informieren**
- **Persönliche Betroffenheit herstellen**
- **Verständnis für technische Sicherheitsbarrieren wecken**
- **IT-Sicherheit als Teil des Jobs verankern**
- **Selbstverantwortung stärken**
- **Kampagne an Unternehmenskultur anpassen**
- **Kein Anrennen gegen „gefährliche“ menschliche Grundeigenschaften wie z.B. Bequemlichkeit oder Hilfsbereitschaft**

Sprache

- **Lieber positiv als negativ formulieren**
- **Lieber Verben als Nomen verwenden**
- **Kurze einprägsame Sätze finden**
- **Lieber persönliche Ansprache „SIE“ als unpersönliches „man“**

Lernziel Blickwendung

<u>Desillusionierung</u> des Benutzerglaubens an

- **Privatheit bzw. Abgeschiedenheit bei der Arbeit am Computer**
- **Direktverbindung mit anderen Menschen über Internet**
- **Exklusive Steuerung der (Arbeits-)Umgebung durch Computeranwendungen**
- **IT-Abteilung (macht die IT „sicher“)**

Positiv formuliert

- **Benutzer weiß dass man ihm stets über Tastatur und Bildschirm schauen könnte**
- **„Schere im Kopf“ bei elektronischer Kommunikation**
  („Könnte meine E-Mail zur Not auch in der Zeitung stehen?“)
- **Sicherer Umgang mit sensiblen Informationen als Teil des Jobs (ggf. Verschlüsseln)**
- **Benutzer kennt seine Abhängigkeiten von integeren IT-Systemen**
- **Eigenverantwortung für Verhalten in einer begrenzt sicheren IT-Umgebung**
- **Akzeptanz von Sicherheitsbarrieren, Werbung für Keepass**

Eye-Opener 1

NDR

Aktuelles aus dem „Alltag“ der IT-Sicherheit

Veröffentlichungen über erfolgreiche Hacker-Angriffe fast schon langweilig:

- Russische Hackergruppe sammelte 1,2 Milliarden Online-Passworte:
  http://www.heise.de/newsticker/meldung/Sicherheitsforscher-Russische-Hacker-erbeuten-1-2-Milliarden-Profildaten-2285655.html
  http://www.n24.de/n24/Nachrichten/Netzwelt/d/5198350/riesiger-datenklau-hinterlaesst-viele-fragen.html
- Masseninfektion von Reise-Websites:
  http://www.proofpoint.com/de/about-us/in-the-news/07132014.php
- Sicherheitslücke beim Musik-Streaming-Dienst Spotify:
  http://www.androidpit.de/spotify-opfer-von-hackerangriff-app-update-schliesst-sicherheitsluecke
- Vision für die nahe Zukunft: Auto-Hacking
  http://www.security-insider.de/themenbereiche/bedrohungen/sicherheitsluecken/articles/454553/
- Überwachte Überwacher:
  http://www.heise.de/security/meldung/Trojaner-Hersteller-FinFisher-wurde-vermutlich-gehackt-2288035.html
- Datenabfluss bei der Steuerakte Uli Hoeneß: Fehlerhafte Zugriffsprotokollierung.
  3000 Zugriffsberechtigte (BR vom 25.8.2014)
- Kreditkartendiebstahl bei vielen UPS-Filialen:
  http://www.golem.de/news/kreditkartendaten-gestohlen-ups-bestaetigt-hackerangriff-1408-108751.html

Eye-Opener 2

NDR

„Online-Spionage wird zur Massenware“ (Handelsblatt vom 24.1.2012)

Preisliste in US$ laut Handelsblatt

- 5$ bis 650$ / Schadprogramm
- 2$ bis 7$ / Shell-Skript als Hacker-Tool
- 1$ bis 20$ / Megabyte E-Mail-Adressen für Spam
- 0,7$ bis 20$ / kompletter Identität (Name, Anschrift, Geburtstag, Konto)
- 1$ bis 18$ / E-Mail-Kennung mit Passwort
- 0,07$ bis 100$ / vollständigem Kreditkartendatensatz
- 0,5$ bis 120$ / gefälschter Kreditkarte mit echten Personendaten
- 10$ bis 900$ / vollständigem Bankdatensatz inkl. Zugangsdaten Online-Banking
- 50$ bis 60$ / 1000 Facebook-Kennungen mit Passwort (Quelle: BKA)

Passwort jeder E-Mail-Kennung angeblich innerhalb von 48 Stunden ermittelbar (ab 150$).

http://www.handelsblatt.com/technologie/it-tk/it-internet/it-sicherheit-online-spionage-wird-zur-massenware/6104226.html

Zusätzliche Lernziele für Führungskräfte

- **Besondere Vorsicht im Umgang mit eigenen Bürodaten**
- **Informationsverantwortung: „Angemessenes“ IT-Sicherheitsniveau definieren (Schutzbedarfsfeststellungen) und bei Benutzern und IT einfordern**
- **Blick auf „Kronjuwelen“, hier unter anderem**
  - **Verfügbarkeit der sende- und sendungsrelevanten Systeme**
  - **Integrität der Sendeinhalte: NDR als Vertrauensanker in der Bevölkerung erhalten**
  - **Integrität und Verfügbarkeit der Onlineangebote (tagesschau.de und ndr.de)**
  - **Zunehmend wichtig: Community-Daten auf sozialen Medien**
  - **Vertraulichkeit von Redaktionsdaten, insbesondere von Informantendaten**
  - **Integrität der Finanz- und Planungsdaten**
  - **Verantwortung für risikomindernde Maßnahmen (z.B. manuelle Kontrollen)**

Fachlicher Inhalt der Informationskampagne

Für alle:

- **Was ist IT-Sicherheit? Was ist IT-Sicherheitsmanagement?**
- **Dienstanweisung IT-Sicherheit im NDR**
- **Benutzerleitfaden zur IT-Sicherheit**

Für Führungskräfte außerdem Empfehlungen zur IT-Sicherheit beim Einsatz von Cloud Computing

Für IT-Bereiche weitere Einzelkonzepte, z.B. Leitfaden für IT-Projektleiter, Checkliste Webanwendungen

Verwendete Medien

- **Kurzvorträge auf Leitungsebene**
- **Testimonials im Intranet**
- **Hauszeitung**
- **Präsenzveranstaltungen auch in externen Standorten**
  (mit Begleitung durch Bereichsbeauftragte)
- **Inhalte auf ständig abrufbaren Intranet-Seiten**
- **Online-Kurs**
- **Flyer: „Die wichtigsten Regeln zur IT-Sicherheit im NDR“**
- **Gehaltsabrechnung zur Verteilung der Flyer an alle**

Andere unternehmensinterne Kampagnen

Vorherige Kampagnen

- **Allgemeines Gleichbehandlungsgesetz (Pflicht zur Teilnahme an Präsenzveranstaltungen oder Online-Schulungen)**
- **Allgemeiner Verhaltenskodex (Medien: Hauszeitung, Intranet, Infokarte)**
- **Kommunikation der Social Media Guidelines im NDR (Medium: Intranet; Später Mitbehandlung in IT-Sicherheit)**

Danach Compliance-Kampagne
(Medien: Hauszeitung, Intranet und Online-Kurs)

Zielsetzung erreicht?

- ✓ **Hohe Aufmerksamkeit für IT-Sicherheit auf Managementebene**
- ✓ **Hohe Sensibilisierung im IT-Bereich**
- ✓ **Ca. 25 % der Festangestellten direkt erreicht**
- ✓ **IT-Sicherheitsbeauftragter als Ansprechpartner etabliert**
- ✓ **Bringschuld des Arbeitgebers erfüllt**
- ✓ **Ausreden bei Fehlverhalten gibt es nicht mehr**
- ✓ **Kaum Vorkommnisse**

Nachhaltigkeit: Ansprache der Benutzer

- **Periodische Schulungen** in Kooperation mit dem Datenschutzbeauftragten (Programmvolontäre, Aufnahmeleitervolontäre, Auszubildende, neue Mitarbeiter)
- **Immer wieder Hauszeitungsartikel und Intranet-Teaser** zu aktuellen Themen (z.B. PRISM und die Folgen)
- **Intranet:** Benutzerleitfaden zur IT-Sicherheit und IT-Sicherheitskonzept
- **Regelmäßige Aktualisierung** aller Dokumente, insbesondere des Benutzerleitfadens zur IT-Sicherheit
- **Online-Schulungsangebot ständig verfügbar**

Nachhaltigkeit: Sensibilisierung durch Schutzbedarfsfeststellungen

- **Schutzbedarfsfeststellungen bei neuen Projekten obligatorisch (gemäß BSI-Grundschutz, auf Rundfunkbelange angepasst)**
- **erinnern die Fachbereiche an ihre Informationsverantwortung**
- **Vereinbarung von Sicherungsmaßnahmen bei hohem Schutzbedarf**
- **Zeitbedarf ca. 1 Stunde pro Projekt, gute Akzeptanz**

Nachhaltigkeit: Sensibilisierung durch Meldepflicht von Vorfällen

- **Meldepflicht von IT-Sicherheitsvorfällen an Vorgesetzte**
- **Weitermeldung an Datenschutzbeauftragten und IT-Sicherheitsbeauftragten**

Regelmäßige Managementberichte

- **Jahresbericht an die Leitung des Hauses**
- **1 Seite Zusammenfassung**
- **2 Seiten Einzelthemen**

Umgang mit den Auswirkungen der Snowden-Veröffentlichungen

- **Haben die Desillusionierung unterstützt**
- **Aber auch Resignation verbreitet**
- **Kommunikation in NDR Hauszeitschrift:**
  „Keine Chance gegen Geheimdienstüberwachung, da bei IT-Sicherheit von Herstellern abhängig“
- **Konsequenz:**
  Bevorzugung persönlicher Kommunikation ohne IT
- **Schutzmöglichkeiten gegen Vielzahl anderer Gefährdungen!**

Karl-Jürgen Hanßmann
k.hanssmann@ndr.de