Kapitel 2: Social Engineering

2: Social Engineering Angriffe

- Social Engineering (soziale Manipulation): Angriffe richten sich nicht direkt auf technische Systeme, sondern auf ihre Benutzer. Ziele sind z.B.
  - Informationsgewinnung (Vertraulichkeit)
  - Benutzer führt vom Angreifer gewünschte Aktionen aus (Integrität)

- Beide Angriffsarten ergänzen sich und können überlappen:
  - Per Massen-E-Mail verschickte Phishing-Versuche
  - Trojanische Pferde locken mit vordergründiger Nutzfunktionalität
  - ...

- Social Engineering ist schwarze (verbotene) Rhetorik

Funktionsweise von Social Engineering

- Ausnutzung menschlicher Eigenschaften, u.a.:
  - Hilfsbereitschaft (z.B. Tür aufhalten)
  - Vertrauen (z.B. Umgang mit Personen in bestimmten Funktionen)
  - Angst (z.B. Drohungen, körperliche Gewalt)
  - Respekt vor Autorität (z.B. Wirkung von Uniformen)
  - Neugierde, Faulheit, Überraschungseffekt, Scham, Schuldgefühl, Zorn, Stolz, Neid, Narzissmus, Mitleid, ...
- Jede menschliche Schwäche kann ausgenutzt werden.
- Social Engineering gibt es immer und überall:
  - Eltern, Erzieher, Lehrer, Freundeskreis, Chef und Kollegen, Partner, ...
  - Werbung, Autoverkäufer, gesellschaftliche Normen, ...
- Bei IT-Sicherheit wird oft primär an Technik gedacht, aber zu wenig an den “Faktor Mensch”.

2.1: Beispiele: Soziale Netzwerke (1/2)

Robin Sage (2010)

- Social Media Profile bei Facebook, LinkedIn, Twitter, . . . 25 Jahre, Master-Abschluss vom MIT
- IT-Sicherheitsberaterin mit 10 Jahren Berufserfahrung
- Job-Angebote u.a. von Google und Lockheed Martin

- Kontaktaufnahme mit 300 Personen:
  Andere IT-Sicherheitsexperten, Mitarbeiter von Rüstungsfirmen und Behörden, hochrangige Offiziere, . . .
- Diverse Aufträge mit Zugang zu vertraulichen Dokumenten, Informationen über Bankkonten, Truppenstandorte, . . .
- Diverse Einladungen zum Abendessen ;-)

Soziale Netzwerke (2/2)

- **Robin Sage ist ein Fake:**
  Experiment von Thomas Ryan zur Vertrauensseligkeit in Social Networks
- Operation „Robin Sage“ ist eine vierwöchige Übung für US-Spezialeinheiten („unconventional warfare exercise“).

Geburtstagsgrußkarte

Elektronische Geburtstagsgrußkarte

- Zwei Angestellte erwähnen Geburtstag ihres Chefs auf Facebook.
- Angreifer schickt E-Grußkarte im Namen eines der beiden.
- Link in E-Mail verweist auf Malware; Rechner vollständig kompromittiert.

Emily Williams (1/2)

Emily Williams, 2012

- 28 Jahre alt, MIT-Abschluss, 10 Jahre Berufserfahrung
- Eigentlich Kellnerin eines Restaurants in Behördennähe

- Innerhalb von 24h nach Anlegen des Facebook-Profils:
  - 60 Facebook-Freunde
  - 55 LinkedIn-Bekannte
  - Drei Job-Angebote von anderen Firmen
- Emily bewirbt sich bei der Behörde:
  - Wird eingestellt, neue Kollegen helfen ihr mit Berechtigungen
  - Social Media Seiten ergänzt um Link auf Malware-Weihnachtskarte
  - Java-Exploit kompromittiert diverse Clients

Emily Williams (2/2)

- Casua *Emily Williams* war nur ein bezahlter Penetration-Test:
  - Durchgeführt von *World Wide Technology*
  - Abgestimmt mit der Behördenleitung
- Fazit des Testleiters (Aamir Lakhani)
  The experiment also shows that attractive women get special treatment in the male-dominated IT industry. The majority of individuals who went out of their way to help Emily Williams were men.

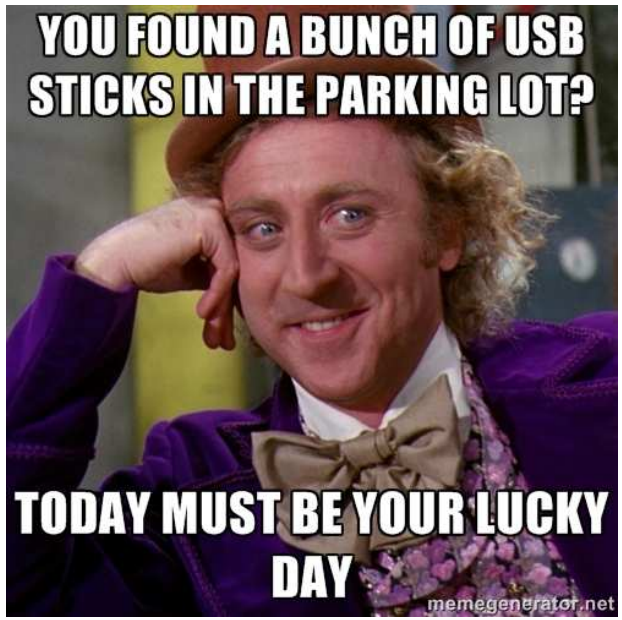
  – Paralleltest mit männlichem Fake-Profil war erfolglos. :)

  > *According to Lakhani, the fundamental problem is that people are trusting and willing to help others. Many also don't think it could happen to them because they don't have an important enough position within an organization, but they don't realize how their actions could help an attacker gain credibility.*

Quelle: `http://www.itworld.com/article/2830438/security/fake-social-media-id-duped-security-aware-it-guys.html`

USB-Sticks

USB-Sticks für Bankangestellte



- Bank beauftragt Security Assessment inkl. Social Engineering
- Bankangestellte wissen, dass auch der Faktor Mensch getestet wird
- 20 USB-Sticks mit Malware auf Parkplatz, Weg zur Kantine, etc. „verloren“
- 15 USB-Sticks werden gefunden, alle 15 werden am Arbeitsplatz ausprobiert

Passwörter Kaufen

- Sailpoint Studie, 2014
  Quelle: `https://www.sailpoint.com/marketpulsesurvey-passwords`:
  Jeder siebte Mitarbeiter (ca 14%) würde seinen Firmenaccount (Benutzername+Passwort) für 150 USD *verkaufen*.

- *Ping Identity* Studie, 2012
  Quelle: `http://www.telegraph.co.uk/technology/internet/9189236/Employees-would-sell-work-password-for-5.html`
  - 48% der Befragten würden Ihren Firmenaccounts für 5 GBP oder weniger zu verkaufen.
  - 30 % der Befragten würden Ihre Firmenaccounts 1 GBP oder weniger verkaufen.

Spear Phishing

Durch *personalierte* Mails/Homepages angelt der Angreifer nach Benutzernamen und Passwörtern Spear Phishing.

Beispiel

- Massenmails an 12.000 Mitarbeitern von 15 Großunternehmen.
- Mail enthielt attraktive Rabatte bei Urlaubsreisen.
- Registierung erfolgt mit den Zugangsdaten des Firmenaccounts.
- 21% der 12.000 *Probanten* registrierten sich bei der Rabattseite mit ihren echten Zugangsdaten.
  - 19 % der geschulten Probanten
  - 24 % der ungeschulten Probanten

Quelle: `http://heise.de/-2461982`

Spear Phishing: Falsche Microsoft-Techniker , 2015

Die Telefonabzocker, die sich als Microsoft-Techniker ausgeben, haben sich eine neue Masche überlegt – und sind jetzt auch telefonisch erreichbar

. . . Im Unterschied zu den von Windows erzeugten blauen Bildschirmen werden dort Support-Rufnummern mit US-Vorwahl angezeigt, über die angeblich der Microsoft-Support erreichbar ist.

Tatsächlich nehmen aber . . . Telefon-Abzocker ab, die mit steigendem Druck nutzlose Service-Dienstleistungen verkaufen wollen. Die Bluescreens werden entweder wenig eindrucksvoll über in Webseiten eingeschleustes JavaScript simuliert oder von einer Adware angezeigt, die man sich im Bundle mit Gratis-Software einfangen kann.

Quelle: `http://heise.de/-2760509`

Spear Phishing: Eigene Erfahrungswerte

Als System Administrator oder Hotlinemitarbeiter ist es relative einfach an Accountdaten von Mitarbeitern zu bekommen.

- Praktisch alle Mitarbeiter verraten der Hotline ihre Accountdaten, wenn ein Problem vorliegt.
- Einig Mitarebiter verraten sogar ungefragt ihre Accountdaten um ein Problem gelöst zu bekommen.

2.2: Kategorisierung

Grundlegende Unterscheidung

- Passive Angriffe (keine Interaktion mit dem Opfer)
  - Belauschen von Gesprächen
  - Beim Tippen „über die Schulter schauen“ (shoulder surfing)
  - Durchsuchen von Papiertonnen (dumpster diving)
  - Liegenlassen präparierter USB-Sticks (baiting)

- Aktive Angriffe (Interaktion mit dem Opfer)
  - Am Telefon als Mitarbeiter der IT-Abteilung oder guter Bekannter/ Assistent des Chefs ausgeben (pretexting)
  - Kontaktaufnahme per E-Mail (phishing)
  - Internet-Bekanntschaften, z.B. über fingiertes Facebook-Konto

Human-based Social Engineering

- Dumpster Diving (Klausurentwürfe in der Papiertonne?)
- Shoulder Surfing (Notebook-Nutzung im Hörsaal?)
- Tailgating (PIN-Code gesicherte Türen)
- Badge Surveillance (Selbstgedruckte Mitarbeiterausweise?)
- Pretexting (Prüfungsamt Angestellte nach dem Passwort Fragen?)
- Quid pro quo (Schokolade für Hausaufgabenblätter?)
- People Watching (Wann verlässt der Dozent sein Büro?)
- Diversion theft (Das Paket können Sie auch mir geben.)

Computer-based Social Engineering

- Phishing
  - Clone phishing (“Update” echter E-Mails)
  - Spear phishing (personalisiertes Phishing)
  - Whaling (Phishing gegen hochrangigen Mitarbeiter)
  - Vishing (Voice Phishing; Ziel: Opfer ruft Angreifer an)
  - Evil Twins (rogue WiFi access points)

- Baiting
  (Im Hörsaal verlorener USB-Stick?)

Gute Social Engineers

- Können gut mit Menschen kommunizieren
  - Harmlose Unterhaltung - Angriff wird gar nicht bemerkt
  - Vortäuschen diverser Stimmungslagen (hektisch, traurig, . . .)
  - Fachjargon des Opfers und seiner Umgebung wird beherrscht
  - Glaubhafte Vertrauensgewinnung oder Positionierung als Autorität
- Sind geduldige Schauspieler
  - Vorgespielte Person muss authentisch wirken
  - Auskundschaften und Vertrauen aufbauen kann dauern
  - Flexiblität und Anpassungsfähigkeit, gutes Faktengedächtnis
- Haben keine Star-Allüren
  - Dumpster Diving macht nicht unbedingt Spaß
  - Tarnung als Reinigungspersonal impliziert entsprechende Tätigkeit

2.3: Gegenmaßnahmen

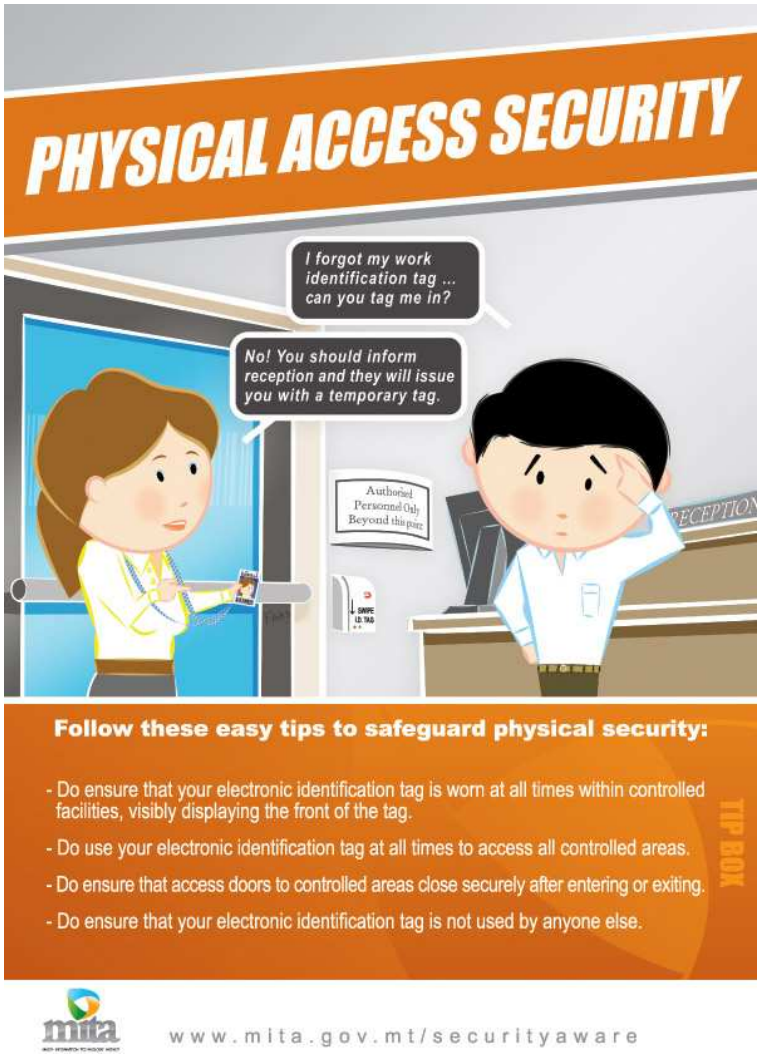
- Leider funktioniert gutes Social Engineering immer.
- Technische Gegenmaßnahmen
  - Dumpster Diving: Aktenvernichtung / Papiertonnen abschließen
  - Shoulder Surfing: Sichtschutzfolien für Notebook-Displays
  - Tailgating: Wachdienst, Vereinzelungsanlagen
  - Baiting: Systeme einschränken, z.B. USB-Ports deaktivieren
- Organisatorische Gegenmaßnahmen
  - Sensibilisieren durch regelmäßige Schulungen, Plakate, . . .

Drei Monate nach der Schulung ist kein Unterschied (in der Reaktion auf die Phishing-Mails) mehr feststellbar

– Enrico Frumento

  - Klare Anweisungen z.B. zu Auskünften am Telefon
  - Meldepflicht für verdächtige Vorkommnisse inkl. Tests

Beispiele für Awareness-Poster

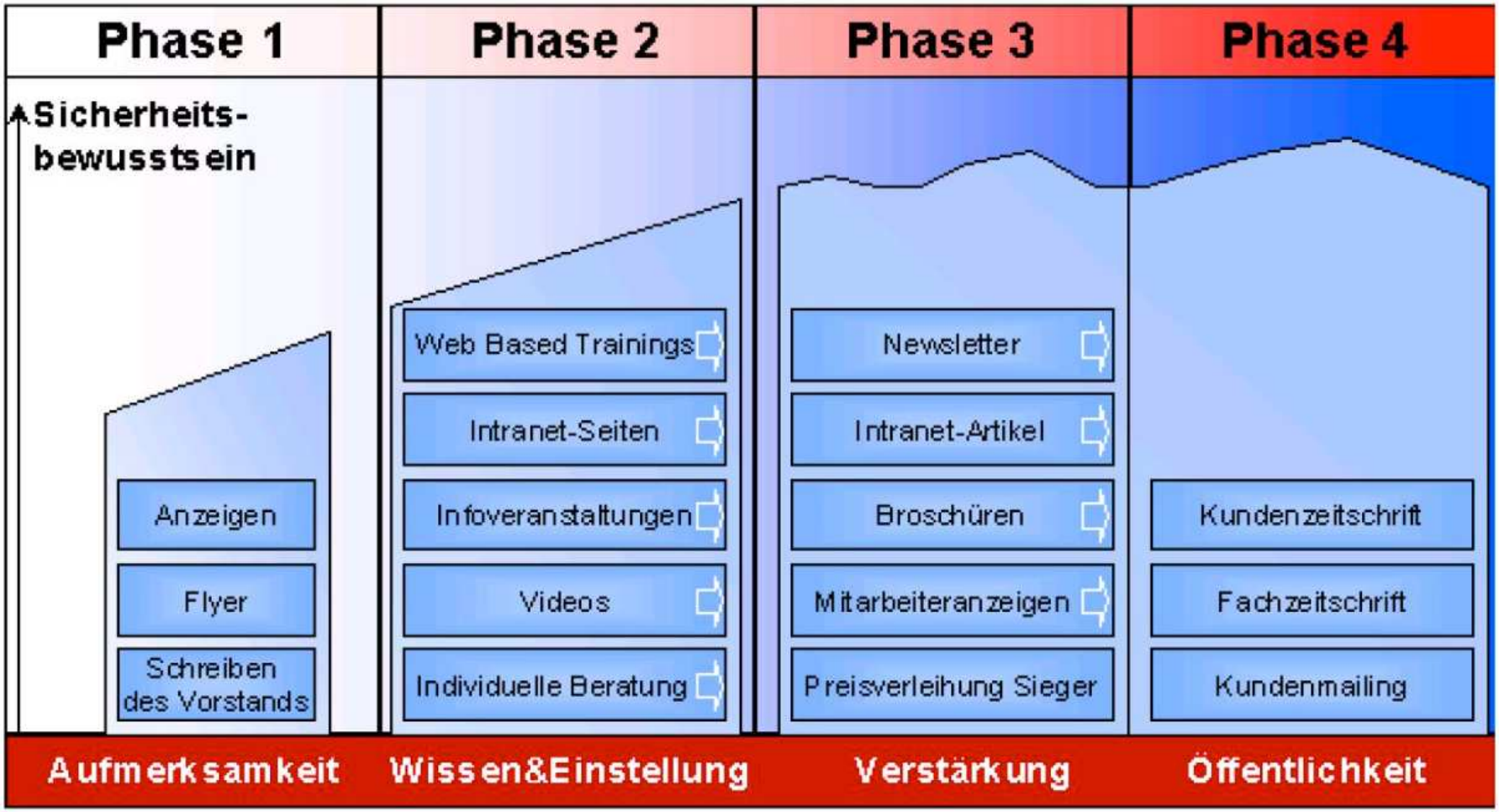


Beispiel für lustige Awareness-Poster

Planung von Awareness-Maßnahmen

- Wie alles rund um IT-Sicherheit auch eine Budgetfrage
  - Personal- und Zeitbedarf für Schulungen
  - Awareness verhindert Schaden, erwirtschaftet aber keinen Gewinn
- Organisatorische Randbedingungen
  - Schutzziele und Schulungsprioritäten müssen definiert sein
  - Inhaltliche, didaktische und mediale Aufbereitung erfordern ein interdisziplinäres Team
  - Kontinuität und Erfolgskontrolle
- Kombination verschiedener Ansätze:
  - Präsenzveranstaltungen vs. Computer-based Training
  - Poster, Flyer, Newsletter, Intranet-Webseiten, ...
  - Bestätigte Kenntnisnahme, Teilnahmezertifikate, Gewinnspiele, ...

Vier-Phasen-Modell nach Fox/Kaun



Quelle: Dirk Fox, Sven Kaun: Security-Awareness-Kampagnen; 9. IT-Sicherheitskongress des BSI, 2005

2.4: Digitale Sorglosigkeit

Die oberste Behörde für die IT-Sicherheit in Deutschland warnt vor wachsenden Bedrohungen im Internet und beklagt eine "digitale Sorglosigkeit" vieler Bürger und Firmen. "Die Angreiferszene rüstet auf", sagt der Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), Michael Hange.

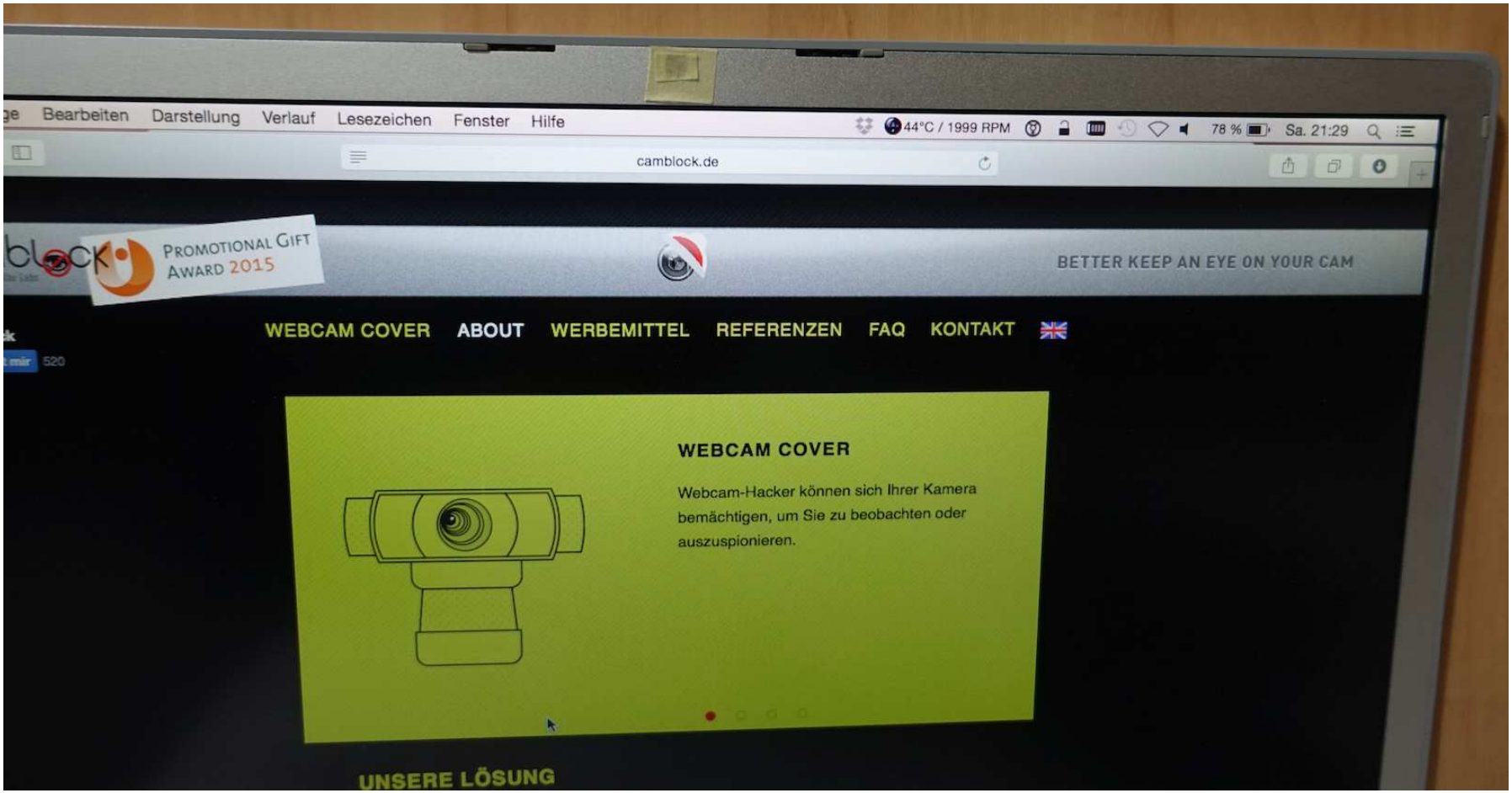
. . . "Viele Nutzer und Firmen merken gar nicht, wenn sie Opfer einer Cyberattacke werden." Zum Teil fehle es an Kompetenz, Gefahren zu erkennen und für genügend Schutz zu sorgen. In vielen Firmen werde außerdem zu wenig in IT-Sicherheit investiert. Gerade bei kleinen mittelständischen Firmen hapere es noch.

Quelle: `http://www.n-tv.de/technik/Eine-Million-deutsche-Computer-infiziert-article14310786.html`

Hauptproblem mangelnde Awareness

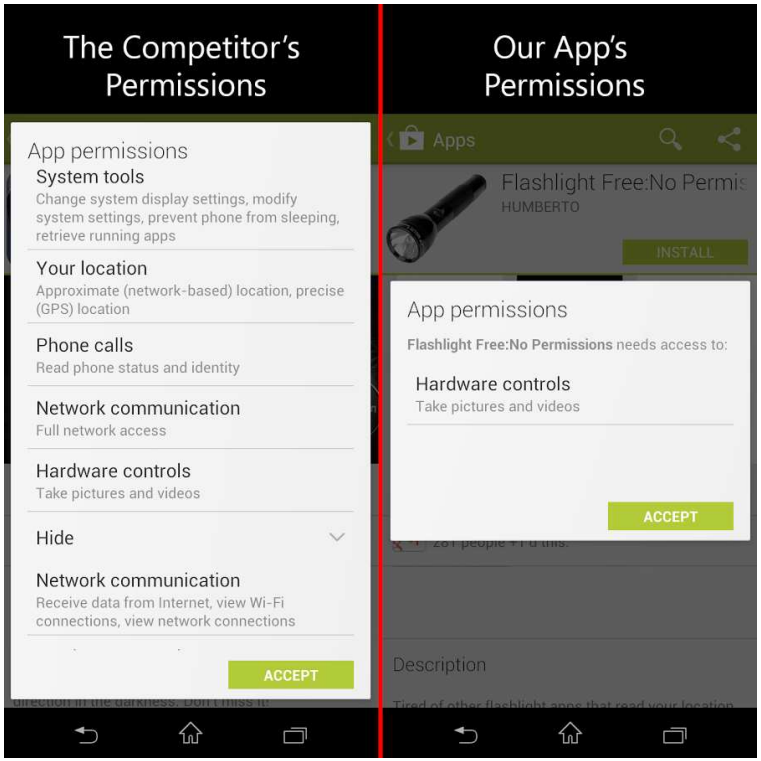
- “Sowas passiert nur anderen.”
- “Warum sollte sich jemand für mich und meine Daten interessieren?”
- “Man kann sowieso nichts dagegen machen.”

Problem 1: Symptome statt Ursachen bekämpfen



Notebook-Webcam verdecken – eine gute Idee?

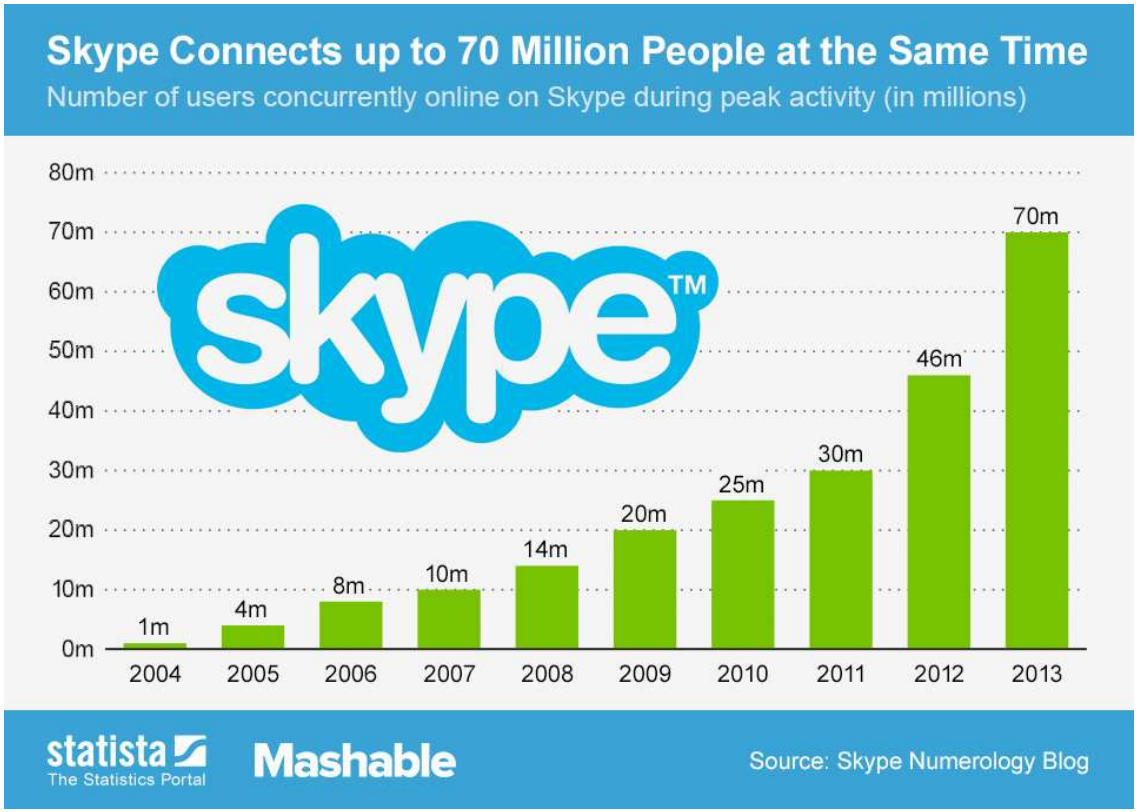
Problem 2: Alles kostenlos, alles ausprobieren



Quelle: `https://play.google.com/store/apps/details?id=com.humberto.flashlight`

Warum braucht ein Taschenlampen-App Zugriff auf GPS, Geräte-ID, WLAN, Photos/Media/Files, USB-Access, Kamera . . . ?

Problem 3: Wider besseres Wissen agieren



Durch Sowden ist seit Juli 2013 bekannt das Skype abgehört wird.

- Snowden-Enthüllungen – Vollständiger Zugang zu Skype (SZ)
- Neue NSA-Dokumente enthüllen die Zusammenarbeit von Microsoft mit der NSA (Telepolis)

Zusammenfassung

Sie sollten . . .

- . . . was man unter Social Engineering versteht.
- . . . die Kategorisierungen von Social Engineering kennen.
- . . . was es an Gegenmaßnahmen gibt.
- . . . verstanden haben was mit *digitaler Sorglosigkeit* gemeint ist.
- . . . wissen das gut gemachte Social-Engineering-Angriffe praktisch immer funktionieren.