Sensibilisierung für Beschäftigte: Pflicht und Chance für Datenschutzbeauftragte

Christian Krause

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

Zu den Aufgaben des Datenschutzbeauftragten zählt…

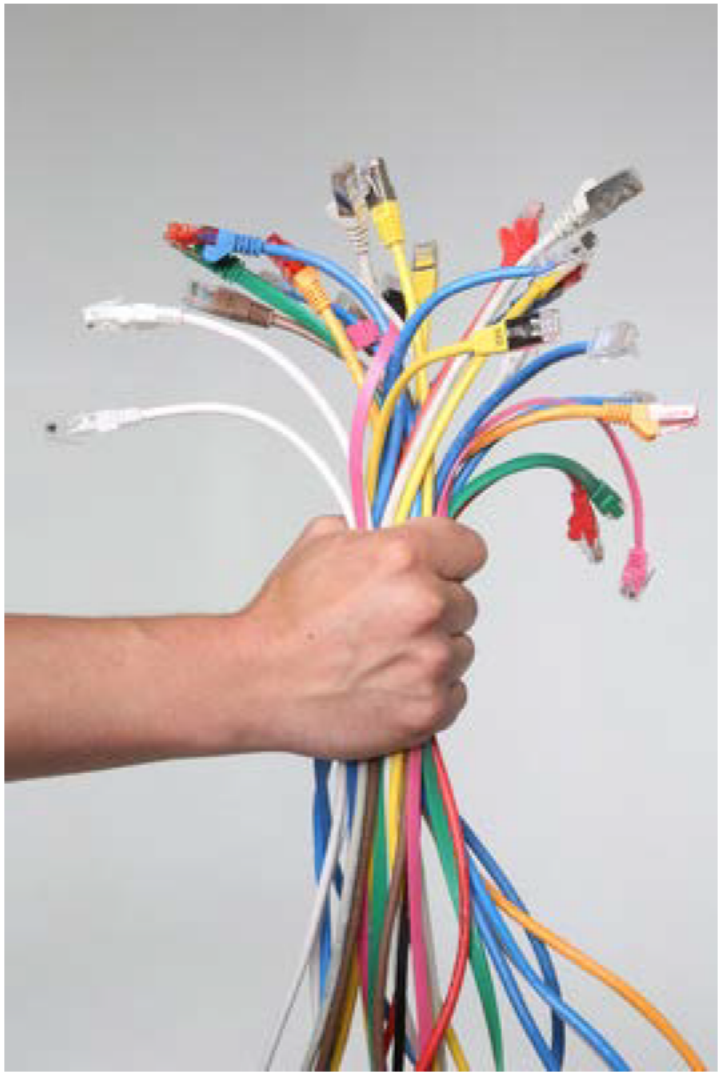
- … Überwachung der Einhaltung dieser Verordnung [DSGVO], […] sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, **der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter** und der diesbezüglichen Überprüfungen;

Sensibilisierung

- Mitarbeitende müssen aufgeklärt werden über
  - Risiken im Umgang mit personenbezogenen Daten
  - Maßnahmen gegen Datenmissbrauch

  - Das kostet Zeit, in der die Mitarbeitenden weder Solitaire spielen noch produktiv sein können.

  → Niemand mag das.



Sensibilisierung

- Datenschutz ist mehr als IT-Sicherheit
- Mitarbeitende dürfen sich nicht auf IT-Maßnahmen verlassen
  (*„Da klick' ich drauf, wir haben ja Virenscanner."*)
- Datenschutzvorfälle können im Ernstfall Kunden kosten, Reputation ruinieren und Bußgelder bescheren

Sensibilisierung: Vorarbeit

- Wie sehen Datenschutz-Konzepte und Dienstanweisungen im Unternehmen aus?
- Wo existieren Reibungsverluste bei der Umsetzung der Konzepte in die Praxis?
- Sind die Konzepte sinnvoll zu praktizieren?

- Datenschutz im Unternehmen ist im Idealfall *„gelebter Soll-Ist-Zustand"*

Sensibilisierung in drei Schritten

1. Problembewusstsein wecken
2. Wissen um Probleme vertiefen und Gegenmaßnahmen vorstellen
3. Gewecktes Bewusstsein langfristig wach halten

Problembewusstsein wecken

- Aufzeigen von möglichen Sicherheits- und Datenschutzrisiken
- Z.B. durch simulierte „Angriffe" auf die Organisation oder Individuen durch Technische Angriffe oder Social Engineering
- Auf ungesperrten Rechnern eine Nachricht in Word hinterlassen, mit [Strg]+[Alt]+[→] den Bildschirm rotieren...
- ..bis hin zu ganzen *„Awareness-Kampagnen"*
- Wettbewerb statt „Anschwärzen":

  Aufklärungskampagnen dürfen nicht zur Diskreditierung einzelner Mitarbeitender führen!
- Nebeneffekt:
  Dokumentation des „Status quo" im Unternehmen

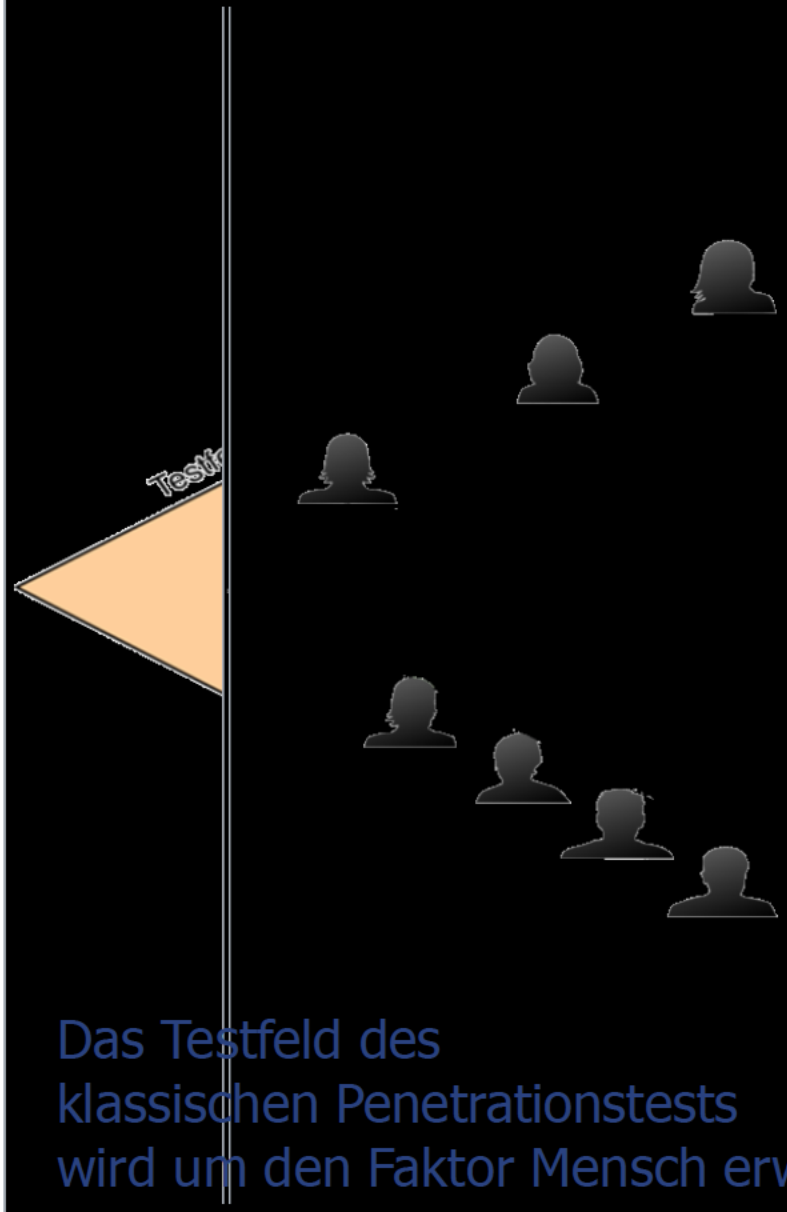
Kiel / Datenschutz-Training 07:00 Uhr / 22.06.2018

Stadt testet Mitarbeiter mit Fake-Mails

Um ihre Beschäftigten stärker für Cyberattacken zu sensibilisieren, hat die Stadt Kiel eine ungewöhnliche Datenschutz-Kampagne gestartet: Sie schickte drei gefälschte Nachrichten an etwa 3000 Mitarbeiter, um ihnen Tricks von Internet-Kriminellen vor Augen zu führen.

Von Martina Drexler

Kiel. Tausende Angriffsversuche auf das Datennetz starten Hacker im Jahr. Die Stadt Kiel konnte sie bisher erfolgreich abwehren. „Hundertprozentige Sicherheit wird es aber auch durch die beste Technik nicht geben. Es ist viel besser, die Mitarbeiter zu sensibilisieren“, begründete der städtische Datenschutzbeauftragte



Das Testfeld des
klassischen Penetrationstests
wird um den Faktor Mensch erweitert.

Quelle: ITS.APT, Universität Bonn

IST.APT : IT-Security Awareness Penetration Testing

- Framework zur Installation einer Testumgebung auf Client-Rechnern
- Clientsoftware kann Ereignisse auf dem Rechner simulieren (sog. Artefakte) und Nutzer-Reaktion darauf aufzeichnen
- Dabei kommen sichere Verfahren zur Pseudonymisierung und Anonymisierung zum Einsatz, so dass die Persönlichkeitsrechte der Probanden gewahrt werden
- Ziel ist es, den *Grad der Awareness* zu ermitteln

- In mehreren Aktionen wurde von einem externen Dienstleister versucht
  - unbefugten Zutritt zu einem Gebäude zu erlangen
  - ungesperrt verlassene PCs zu finden
  - Passworte per Telefon oder Mail zu erfahren
  - Zugriff auf unverschlüsselte Laptops zu erlangen
  - klassifizierte Dokumente zu finden, die ungeschützt herumlagen

Angriffe mit Ankündigung

Was das Phantom zu sehen bekommt…

- Bei demonstrativen, geplanten Angriffen unbedingt **im Vorfeld definieren**, wie mit erlangten Informationen umgegangen wird.
- **Dienst-/Betriebsvereinbarungen** wahren die Mitbestimmungsrechte des Personal- bzw. Betriebsrats
- *Beinahe* erlangte Informationen reichen eventuell aus: Bspw. können telefonische Passwortabfragen rechtzeitig abgebrochen werden, Eingabefelder auf Webseiten können den „Senden"-Knopf ignorieren.

Wissen um Probleme vertiefen und Gegenmaßnahmen vorstellen

Grundlagen im Privaten – Selbstverständlichkeit im Beruf

- Maßnahmen, die auch im privaten Bereich Sinn ergeben, lassen sich leichter und nachhaltiger vermitteln.
  - Passwortsicherheit am Beispiel des privaten eBay-Kontos ist nachdrücklicher als das firmeninterne AD.
  - E-Mail-Sicherheit betrifft nicht nur das dienstliche Outlook, sondern auch das heimische Thunderbird oder das GMX-Konto.
  - Office-Dateien mit Metadaten geben nicht nur Angestellte, sondern auch Privatpersonen weiter.

Der Klassiker: Passworte

- Vor wem soll das Passwort schützen?
  - Entfernter Angreifer
  - Lokale Angreifer

Wie läuft eine Passwortattacke ab?

- Überredungskunst:
  *"**Social Engineering** kostet nichts und überwindet alle technologischen Barrieren, weil es geschickt das Vertrauen und die Neugier der Menschen ausnutzt"* Kevin Mitnick
- **Gezieltes Raten**:
  Haustiere, Kindernamen, Jahreszahlen, Hobbies

- "**Brute Force Attacke**": Ausprobieren
  - Über das Netz
    - Langsam. Auffällig.
  - Auf eine Datei
    - Schnell. Nicht bemerkbar.

Beispielhafter Aufhänger aus dem Privatbereich:

heise Security

News ▾ Hinterg

Security > 7-Tage-News > 09/2018 > Knuddels.de: Millionen Nutzerdaten mit Passwörtern geleakt

Knuddels.de: Millionen Nutzerdaten mit Passwörtern geleakt UPDATE

Stand: 08.09.2018 11:37 Uhr – Martin Holland

Merkbare Passworte

- **B**ob **B**eamon **s**prang **a**ls **e**rster **8,90m.**
- Aber warum eigentlich abkürzen?
- Anhaltspunkt: **Entropiewerte** von
  - BBsae8,90m. 50,2 bit
  - Dinkel Schuh 52,6 bit

Natürlicher Feind von Dinkel Schuh:

Sogenannte "Wörterbuchattacken":
Durchprobieren von Wortlisten.

Passwortattacken
Richtig ist das neue Falsch

- Algorithmen analysieren Lebensumstände, Arbeits- und Sozialumfeld und generieren individuelle Wortlisten: *zwV* im Behördenkontext unsicherer als beim Bäcker
- „Leetspeech" ist überraschenderweise auch den Crackern bekannt. In 3ch7.
- Syntaktische Fehler machen Passworte stark: *Pqasswort*

- ***BBsae8,90m, dank Dinkel Schuh.***

Wo lasse ich meine Passworte?

- In der 1. Phase wurde erarbeitet, dass Räume sicher sein sollten. Daher:
- Wenn die Räumlichkeiten sicher sind, können Passworte aufgeschrieben und dort verschlossen verwahrt werden.
  - *Solange die eigene Hardware (Computer) sicher vor Unbefugten ist, ist es auch der Zettel. Ist der Zettel nicht sicher, ist die Hardware nicht sicher. Und dann nützt das beste Passwort nichts.*
    (→ Hardware-Manipulation/Keylogger)

- Diskutieren Sie Möglichkeiten der Verwendung von Passwort-Safes

Und wuarm stolle man biem E-Mial-Vnaresd uidngbent duaraf aethcn, den rthenicign Efgempänr zu whäeln?

- Da das Gehirn sehr gut mit unsinnigen Zeichenfolgen umgehen kann, sind Schreibfehler bei der Adressierung mitunter schwer zu entdecken.
- Darum: **PÜRF DIE ARSEDSE**!

Regelmäßige Impulse

- Rundschreiben, Newsletter oder ähnliches
- Regelmäßige Aktionen wie in Phase 1 in kleinem Stil
- Anekdoten bzw. konkrete Problemfälle aus der Praxis:
  - Was haben wir während der Hitzewelle mit Türen und Fenstern gemacht?
  - Wie sind wir mit konkreten Datenschutzvorfällen umgegangen?

Diese Pforte..

- ...ist *sicherlich* nicht Teil irgendeines Sicherheitskonzepts.

Vielen Dank!

Christian Krause
ULD38@datenschutzzentrum.de
Tel. 0431-988 1247