FRAMA
mail. message. managed.

DIGITALE KOMMUNIKATION

FRAMA
mail. message. managed.

INHALT

- Aktuelle Lage
- Gedanken zu digitaler Kommunikation
- Einfluss auf betriebliche Prozesse
- Datenschutzgrundverordnung

AKTUELLE LAGE – GEFÄHRDUNG E-MAIL

- Mitlesen
- Überlastung durch eingehende E-Mails
- Falsche Absender
- Aktive Inhalte
- Schadprogramme
- Spam
- Gezielte Angriffe
  - CEO Fraud
  - Whaling
  - Bewerbung

FRAMA
mail. message. managed.

AKTUELLE LAGE – WAS TUN WIR?

- Wer sich mit Informationssicherheit befasst, der kennt Grundsätze wie:
  - Firewall einsetzen
  - Virenscanner installieren und aktuell halten
  - Transferserver in einer DMZ
  - Datensicherungen erstellen
  - Starke und verschiedene Passwörter verwenden
  - Möglichst nur sichere Protokolle verwenden
  - Beim Surfen auf https:// achten
  - Keine Anhänge von unbekannten E-Mail-Absendern öffnen
  - Spam-Filter
  - Monitoring-Systeme
  - …

AKTUELLE LAGE – INNERBETRIEBLICH

- Es wird viel investiert:
  - In Infrastruktur
  - In Managementsysteme
    - Kontrollsysteme
    - Risikomanagement
    - BCM
  - In Prozesse
    - Vier-Augen-Prinzipien
    - Kontrollen
    - Nachvollziehbarkeit
  - Regelwerke
  - …

FRAMA
mail. message. managed.

AKTUELLE LAGE

- Und trotzdem:
  - Mehr als 90% aller E-Mails sind kriminell
  - Weltumspannende Botnetze mit Millionen von Rechnern
  - Stillstand in Netzwerken durch DDoS Attacken
  - Finanzabflüsse durch falsche Rechnungen (nicht nur durch E-Mails)

- Trotz gewaltigen Ausgaben haben wir die noch grösseren Schäden

- Wo können wir noch ansetzen? Was noch tun?

FRAMA
mail. message. managed.

EXKURS «MEIN» TAG

EXKURS «MEIN» TAG

FRAMA
mail. message. managed.

DIGITALE KOMMUNIKATION

- Offensichtlich habe ich bewusst privat und geschäftlich kommuniziert:
  - E-Mail
  - Telefonate
  - Nachrichten versendet
  - Angaben in Facebook etc. aktualisiert

DIGITALE KOMMUNIKATION

- Ich habe aber auch unbewusst kommuniziert:
  - Essgewohnheiten
  - Verkehrslage
  - Wetterbedingungen
  - Standort
  - Kaufverhalten
  - Vorlieben
  - Gesundheitszustand
  - Bevorzugte Sendungen / Sportarten
  - Reiseverhalten und –Ziele
  - …
- Vergleichbar mit der menschlichen Körpersprache, digitaler Fussabdruck

MÖGLICHE FOLGEN – FALL 1

Fall: Mobiltelefon / Fitnessarmband

Für den Lebenspartner

Ist auf Arbeit oder nicht
Treibt gerade seinen Sport (auch horizontalen)

Erst recht dann, wenn Sie vorsichtig sind und Ihr Armband mal ablegen und das Mobiltelefon ausmachen…

Für die Krankenversicherung

Bewegt sich genügend / ungenügend
Betreibt zu viel Extremsport
Ist ein Risiko-Patient, Versicherungsprämie zu günstig

MÖGLICHE FOLGEN – FALL 2

Fall: Kundenkarte Lebensmittelkette

Schwangerschaft

Die Lebensmittelkette weiss durch geändertes Kaufverhalten drei Wochen vor der Frau, dass diese schwanger ist…

Partnerschaft

Die Lebensmittelkette weiss mit 85% Wahrscheinlichkeit, ob ein Paar in einem Jahr geschieden sein wird oder nicht. Erst recht dann, wenn beide heute davon noch nichts wissen und daher auf ihr Verhalten nicht achten…

DIGITALER FUSSABDRUCK

- Tägliche Informationspreisgabe
- Nachhaltig
- Rückschlüsse auf Wahrheiten
- Stark beeinflussbar

INNERBETRIEBLICH

- Jegliche digitale Kommunikation macht uns angreifbar
  - Z.B. Personalisierte E-Mails an HR mit Bewerbungsunterlagen
  - Z.B. CEO Fraud
  - Whaling

- Was sich ein Social Engineer vor 10 Jahren mühsam erarbeiten musste, steht ihm heute im Netz zur freien Verfügung

- Dass sich jemand mit krimineller Absicht digitale Informationen beschafft, bemerken wir in der Regel nicht

DATENSCHUTZ

- Natürliche Personen geniessen abgeleitet aus den Menschenrechten ein Grundrecht auf Schutz ihrer Daten

- Datenschutz soll Menschen und deren Recht auf informationelle Selbstbestimmung schützen
  - Selbst entscheiden, wem wann welche persönlichen Daten zugänglich sind

- Datenschutz will den unfreiwillig «gläsernen Menschen» durch eine faire und transparente Datenverarbeitung verhindern

DSGVO ECKPUNKTE

- Informierte Einwilligung zur Datenverarbeitung
  - Betroffener muss umfassend und verständlich informiert sein
  - Betroffener muss explizite Zustimmung gegeben haben
  - Betroffener kann Zustimmung jederzeit zurückziehen
  - Vertrag darf nicht an Verarbeitung von Daten gebunden sein
    - Stichwort: Wettbewerbsteilnahmen zur Datenerhebung
    - Stichwort: Kundenkarte zwecks Rabatterteilung

- Auskunfts- und Berichtigungsrecht
  - Anfragen zum Datenbestand müssen rasch und kostenfrei beantwortet werden
  - Falsche Daten sind umgehend zu berichtigen

DSGVO ECKPUNKTE

- Data protection by Design
  - Systeme datenschutzkonform auslegen
  - Möglichst wenige Daten sammeln
  - Nur solange wie unbedingt nötig speichern
    - Achtung Aufbewahrungsvorschriften anderer Gesetze
  - Dem Betroffenen die Kontrolle über seine Daten ermöglichen

- Data protection by Default
  - Systeme müssen datenschutzfreundliche Voreinstellungen haben
    - Beispiel: Einstellung Facebook zur Öffentlichkeit des Profils

FRAMA
mail. message. managed.

DSGVO ECKPUNKTE

- Recht auf Vergessen
  - Betroffene haben das Recht Daten löschen zu lassen
    - Achtung: Gesetzliche Forderungen nach Speicherung
    - Achtung: Datensicherung
    - Achtung: An Dritte weitergegebene Daten

- Schutz der Daten
  - Nach Art und Umfang der Verarbeitung sind dem Risiko angemessene organisatorische und technische Sicherheitsmassnahmen nach Stand der Technik zu treffen

  - Risikoanalyse des ISMS mit Datenschutzaspekten ergänzen, regelmässig aktualisieren

DSGVO ECKPUNKTE

- Nachweiserbringung
  - Nachweise zur Einhaltung von Regelungen und Massnahmen zum Datenschutz sind zu erbringen.
    - Achtung: Protokollierung / Überwachung von Mitarbeitenden
  - Regelungen und Massnahmen sind regelmässig zu prüfen
    - Stichwort: Internes Audit
- Verzeichnis von Verarbeitungstätigkeiten
  - Wo sind welche Daten zu welchem Zweck wie lange gespeichert
  - Kontaktdaten des Verantwortlichen

DSGVO UMSETZUNG, STRAFBEWEHRUNG

- Seit Mai 2016 in Kraft
- Muss bis zum Mai 2018 umgesetzt sein
- Strafbewehrt bis zu 20 Mio. oder 4% des Umsatzes, beachtet wird der höhere Wert.

ZUM NACHDENKEN

- Wissen Sie persönlich:
  - Wem Sie die Verarbeitung von Daten erlaubt haben?
  - Was dieser mit den Daten anstellt und welche Daten er über Sie hat?
  - Wo und welche Daten Sie heute bekannt gegeben haben?
  - Was über Sie im Internet zu finden ist?
  - Warum Sie nach einer ausgiebigen Produktrecherche im Internet per Mail äusserst passende Werbung erhalten?
  - …

FRAMA
mail. message. managed.

ZUM NACHDENKEN

- Weiss Ihre Organisation / Unternehmen:
  - Welche personenbezogenen Daten verarbeitet werden?
  - Wo diese Daten, von wem und wozu bearbeitet werden?
  - Wie und für welche Dauer diese Daten gespeichert sind?

- Kann Ihre Organisation / Unternehmen:
  - Auskunft geben über den kompletten Datenbestand einer bestimmten Person?
  - Datenbestände einer bestimmten Person auf Löschbarkeit prüfen und gegebenenfalls auch löschen?
  - Nachweise erbringen, dass personenbezogene E-Mails nur verschlüsselt versandt werden?

INNERBETRIEBLICHE SCHLUSSFOLGERUNG

- An der Umsetzung der DSGVO dringend arbeiten
- Daraus lernen und sensibel im Umgang mit Daten werden
- Mitarbeiter sensibilisieren
- Digitalen Fussabdruck der Organisation wahrnehmen und bewusst werden, was wir als Organisation über uns bekannt geben

FRAMA
mail. message. managed.

VIELEN DANK
FÜR IHRE AUFMERKSAMKEIT

Mark Schilt
Chief Information Security Officer
Frama AG
mark.schilt@frama.com