I don‘t wanna cry

Datenschutz in Redaktionen

Gliederung

- I don`t wonna Cry, Datenschutz in Redaktionen
- Bedrohungslage
- Wanna Cry
- Datensicherheit
- Social Engineering
- Phishing
- Schwachstellen
- Cloudsysteme
- Was Sie sonst noch tun können

Bedrohungslage

Täglich werden ca. 380.000 neue Schadprogrammvarianten gesichtet

In 2016 waren insgesamt mehr als 560 Millionen verschiedene Schadprogrammvarianten bekannt

Das Entdeckungsrisiko ist für die Täter eher gering

Angriffe werden zielgerichteter und sind sehr gut vorbereitet

Schadcode wird intelligent

Selbst einfache Makroviren erkennen heute, ob sie in einer Analyseumgebung ausgeführt werden.

Angriffe laufen auf allen erfolgversprechenden Plattformen

IT/Administratoren

- Sollen primär die Geschäftsprozesse unterstützen
- Sind verantwortlich für die IT Sicherheit
- Sollen auch den Datenschutz/Datensicherheit beachten
- Stetig kommen weitere Aufgaben dazu
- Personal bleibt aber gleich, oder verringert sich
- Budgets bleiben meist unter den Erwartungen
- Müssen Störungen nach Prioritäten abarbeiten
- Soll kosten in der IT senken

User

- Möchte Störungsfrei seine Arbeit erledigen
- Nutzt dafür DV-Systeme
- Wünscht keine Veränderungen (Upgrades)!
- Ist sich seiner eigenen Gefährdungssituation nicht bewusst
- Versteht die IT Zusammenhänge oft nicht
- Besitzt unwissentlich aber eine Schlüsselfunktion hinsichtlich der IT Sicherheit

Wanna Cry

- Gibt aktivem Konto Windows-Konto Adminrechte
- verschlüsselt etwa 100 Dateien mit 2048-BIT RSA Key
- Dateien erhalten die Endung *.WNCRY
- Verbreitete sich nicht per Mail sondern via SMB-Schnittstelle
- Nutzte Sicherheitslücke im NetBios
- Verursacher wohl Equation Group
- NSA informierte MS erst, als Eternal Blue gestohlen wurde
- „Erlöse" aus Wanna Cry weltweit ca. 93T€ (Quelle Handelsblatt)
- Schaden aber weit höher

Datensicherheit

- Größtes Risiko sind E-Mail-Anhänge und Drive-by Downloads
- Zur Verbreitung von Ransomware wird überwiegend Phishing eingesetzt.
- 73% der Malware geht auf Phishing zurück
- Ransomware "Locky, und TeslaCrypt weiter auf Wachstumskurs

Datensicherheit

- Es gibt nur 2 Möglichkeiten
- in ein System einzudringen
- - technisches Versagen
- - menschliches Fehlverhalten

Social Engineering

- Angriffe richten sich nicht direkt auf technische Systeme, sondern auf ihre Benutzer.
- Bei IT-Sicherheit wird oft primär an Technik gedacht, aber zu
- wenig an den "Faktor Mensch".
- ... Social Engineering kostet nichts und überwindet alle technologischen Barrieren ...– *Kevin Mitnick*
- Sicherheitsexperten sehen daher in Social Engineering die größte Gefahr für jedes Sicherheitssystem

Social Engineering

- in Notsituationen unbürokratisch zu helfen
- auf Hilfe mit Gegenhilfe zu reagieren
- störungsfreie Abläufe zu gewährleisten
- materiellen Gewinn zu erzielen
- sich vor der Führungskraft auszuzeichnen

- Arbeitsabläufe zu behindern und damit Schaden anzurichten
- vor der Führungskraft schlecht dazustehen
- einen wichtigen Kunden (durch Unwissenheit) nicht angemessen zu behandeln und vielleicht zu verlieren
- unseren Mitmenschen nicht zu gefallen

Social Engineering

- Grundlegende Unterscheidung:

- Passive Angriffe (keine Interaktion mit der Zielperson)
- Aktive Angriffe (Interaktion mit der Zielperson)

- Passive Angriffe sind z.B.

- Belauschen von Gesprächen
- Beim Tippen „über die Schulter schauen" (shoulder surfing)
- Durchsuchen von Papiertonnen, (dumpster diving)
- liegenlassen präparierter USB-Sticks (baiting)

Social Engineering

- Aktive Angriffe:
- Am Telefon als Mitarbeiter der IT-Abteilung ausgeben (pretexting)
- Mit VOIP lassen sich Vorwahlen und Rufnummern einfach faken
- Kontaktaufnahme per E-Mail (phishing)
- Internet-Bekanntschaften, z.B. über fingiertes Facebook-Konto

- Human-based Social Engineering (ohne technische Hilfsmittel)
- Computer-based Social Engineering (mit technischen Hilfsmitteln)
- Reverse Social Engineering (Opfer wendet sich freiwillig an Angreifer)

Social Engineering

- **Ziele sind z.B.**

- Informationsgewinnung (vs. Vertraulichkeit)
- Benutzer führt vom Angreifer gewünschte Aktionen
- aus (vs. Integrität)
- Schaden verursachen (vs. Verfügbarkeit)
- Identitätsdiebstahl
- Image- oder Rufschädigung
- Erpressung
- Zugriff auf weitere Datensysteme

- Hauptziel sind Passwörter!

Computer Based SE

- Phishingformen

- Clone phishing (“Update” echter E-Mails)
- Spear phishing (personalisiertes Phishing)
- Whaling (Phishing z.B. gegen hochrangigen Mitarbeiter)
- Vishing (Voice Phishing; Ziel: Opfer ruft Angreifer an)
- Evil Twins (WiFi access points)
- Baiting gefundener USB-Stick?

Beispiel SE in SM

- Robin Sage (2010, Thomas Ryan)

- Social Media Profile bei Facebook, LinkedIn, Twitter, ...
- 25 Jahre, Master-Abschluss vom MIT
- IT-Sicherheitsberaterin mit 10 Jahren Berufserfahrung

- Kontaktaufnahme mit 300 Personen:
- Andere IT-Sicherheitsexperten, Mitarbeiter von
- Rüstungsfirmen und Behörden, hochrangige Offiziere,
- Job-Angebote u.a. von Google und Lockheed Martin
- Diverse Aufträge mit Zugang zu vertraulichen Dokumenten, Informationen über Bankkonten, Truppenstandorte,

Social Engineering

- Mitarbeiter eines Unternehmens werden mit einem Trick überredet, die normalen Sicherheitsvorkehrungen zu umgehen und sensible Informationen preiszugeben.
- Sicherheitsexperten sehen in Social Engineering die größte Gefahr für jedes Sicherheitssystem
- Stetig wachsende Zahl von E-Mails, Sozialen Netzwerken und anderen Kommunikations-plattformen

Social Engineering

- Je nach Zielsetzung und Fähigkeiten eines Angreifers können
- Social-Engineering-Angriffe einfacher und effektiver sein als
- technische Angriffe.

- Teilweise gibt es technische Gegenmaßnahmen; ansonsten
- sind Awareness-Maßnahmen der beste bekannte Ansatz.

- Gute gemachte Social-Engineering-Angriffe funktionieren immer und überall!

Social Engineering

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Anmelden

Menü | Politik Meinung Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft mehr▾

NETZWELT Schlagzeilen | Wetter | DAX 12.162,70 | TV-Programm | Abo

Nachrichten > Netzwelt > Web > Internetbetrug > Betrug per E-Mail: US-Manager überweist 15 Millionen Euro nach China

Gefälschte E-Mails

US-Manager überweist 17 Millionen Dollar an Betrüger

Mit gefälschten E-Mails haben Internetbetrüger einen amerikanischen Top-Manager dazu gebracht, umgerechnet 15 Millionen Euro auf ein Bankkonto in China zu überweisen. Das Opfer glaubte, auf Anweisung seines Chefs zu handeln.

The Scoular Company — Count on Scoular People — Search

Products & Services

MARKETS WE SERVE | PRODUCTS & SERVICES | OUR LOCATIONS | CAREER OPPORTUNITIES | ABOUT SCOULAR | NEWS RELEASES | CONTACT US

Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Von: Amazon Support <mailer@fsafd.xyz> Gesendet: So 10.09.2017

An:

Cc:

Betreff: Ihre Zahlung wurde abgelehnt.

Ihre Bestellung über 1.121,21€ bei Microsoft wurde storniert.

Die Prüfung Ihrer Bestellung hat ergeben, dass diese Transaktion möglicherweise nicht von Ihnen autorisiert wurde. Zum Schutze Ihrer persönlichen Daten, wurde Ihr Amazon-Konto vorübergehend gesperrt.

Um wieder mit Ihrem Amazon-Konto einkaufen zu können, ist eine Überprüfung Ihrer Identität erforderlich.
Loggen Sie sich hierzu über den unten stehenden Link ein und folgen Sie den Anweisungen.

Einzelheiten Ihrer Bestellung

Bestellung: #123-1447215136-458875899

Aufgegeben am 06. September 2017

Microsoft Surface Pro 4 31,24 cm (12,3 Zoll) Tablet-PC (Intel Core i5, 8GB RAM, 256GB, Intel HD Graphics, Windows 10 Pro) **EUR 1.121,21**

Zustand: Neu
Verkauft von: Microsoft
Versand durch: Amazon

Zwischensumme: EUR 1.111,21
Verpackung und Versand: EUR 0,00

Endbetrag: EUR 1.121,21
Gewählte Zahlungsart: Kreditkarte

Anschließend werden sie zur Amazon Konfliktlösung weitergeleitet, um die Einschränkungen

Ein Paradebeispiel

SE Gegenmaßnahmen

- Beispielmaßnahmen:

- Technisch:
- Dumpster Diving Aktenvernichtung / Papiertonnen abschließen
- Shoulder Surfing Sichtschutzfolien für Notebook-Displays
- Baiting : Systeme einschränken, z.B. USB-Ports deaktivieren

- Organisatorisch:
- Sensibilisieren durch Schulungen, Plakate, Übungen,
- Klare Anweisungen z.B. zu Auskünften am Telefon
- Meldepflicht für verdächtige Vorkommnisse inkl. Tests

Maßnahmen gegen SE

- 1. Seien Sie zurückhaltend bei Auskünften
- 2. Lassen Sie sich nicht unter Druck setzen
- 3. Haben Sie den Mut, ein Gespräch zu beenden
- 4. Überprüfen Sie die Identität des Anrufers
- (z.B. durch einen Rückruf)
- 5. Achten Sie auf sensible Dokumente
- 7. Sprechen Sie fremde Personen im Unternehmen an
- 8. Sicherheit geht vor Höflichkeit
- 9. Die Offenbarung eines Fehlers darf nicht bestraft werden

Maßnahmen gegen SE

- Regelmäßige Schulungen der MA
- Keine vertraulichen Gespräche an öffentlichen Orten
- Vorsicht in sozialen Netzwerken
- Vorsicht bei E-Mails und Dateianhängen
- System Hardening
- Clean Desk/Clear Screen Policy
- Security-Awareness-Kampagnen erhöhen das
- Sicherheitsbewusstsein

Maßnahmen gegen Phishing

Prüfen Sie die URL, bevor Sie darauf klicken

Beachtung des „www" Bereiches

https://ich.kann.vor.dem.www.bereich.so.viele.Punkte.setzen.wie.ich.möchte.amazon.de)

Name außerhalb des „www" Bereiches
(www.amazon.de.shoppen.im.internet.de

Prüfen Sie den „www" Bereich auf Tippfehler und ähnlich aussehenden Zeichen (www.mediarnarkt.de)

Nutzen Sie TORPEDO
(https://www.secuso.informatik.tudarmstadt.de/de/secuso/forschung/ergebnisse/torpedo/

Schwachstellen

- Datenmüllentsorgung

- Datenspeicher in Druck-
- und Kopiersystemen

Cloudsysteme

- Norm für Cloudsysteme ist die ISO 27018
- Setzt auf ISO 27001 auf
- verlangt Benachrichtigungs-, Informations-, Transparenz- und Nachweispflichten
- Provider müssen Prozesse festlegen, die die Rückgabe, Übermittlung, Transfer und Vernichtung von pb Daten nach Vertragsende festlegen.
- Ist auf den Schutz pb Daten fokussiert
- Funktioniert mit Audio, Bildern und Text
- „gekapseltes" System außerhalb der IT Infrastruktur

Mailverkehr

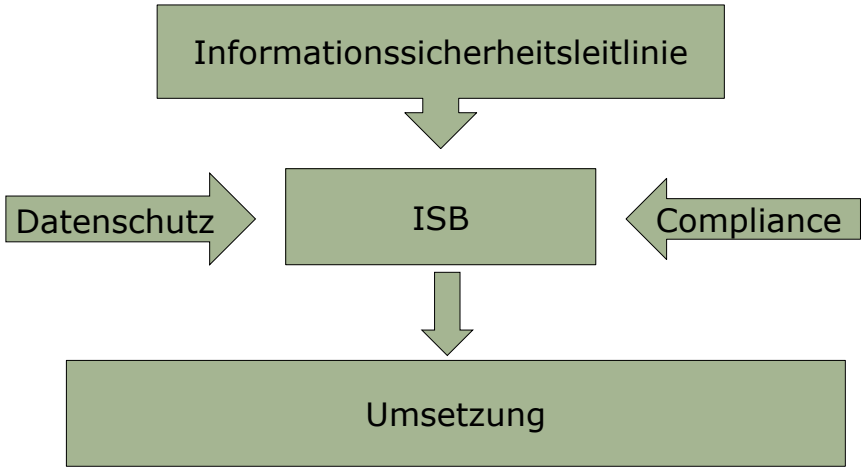
- Verschlüsselung für externe Mails meist nicht umsetzbar, weil zu komplex und zeitaufwändig
- Alternativ Schlüsselaustausch über Cloudsysteme
- PDF Dokumente vor dem Versenden mit einem Passwort versehen. Passwort in separater Mail oder als SMS versenden.

Was Sie sonst noch tun können

- § 3a BDSG Datenvermeidung
- TOR Netzwerk nutzen
- Passwortmanager verwenden
- Verschlüsselung von Festplatten (BitLocker)
- Achten Sie auf Datenschutz in mobilen Endgeräten
- Einsatz von Redaktionssystemen
- Leben Sie das PDCA Modell
- Erarbeiten Sie einen Notfallplan mit Ihrer IT

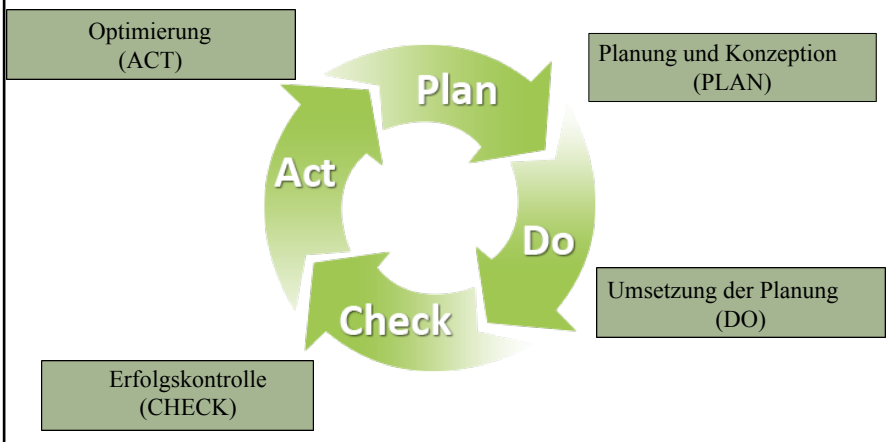
- Und vor allem…

Informationssicherheit

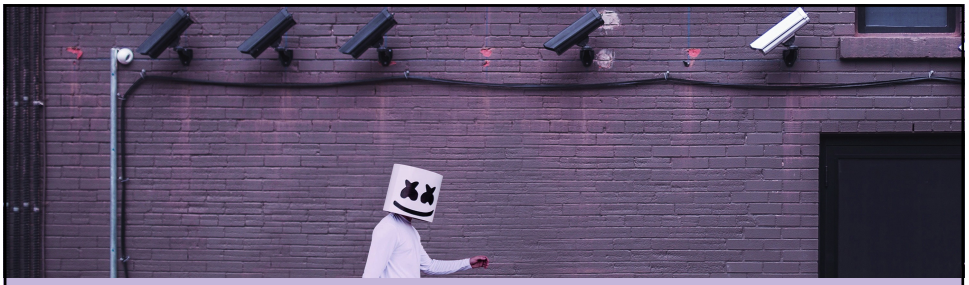


Lernen Sie IT!

PDCA-Modell nach Deming



Bleiben Sie auf dem Laufenden



DS2018 Gesellschaft für Datenschutz und Datensicherheit GmbH

Sommerbergstraße 97
66346 Püttlingen
Regionalverband Saarbrücken
Telefon 06806/4999529
Telefax 06806/920294
E-Mail info@ds2018.de