Informationssicherheit, Datenschutz, Urheberrecht

ISDS

Themenübersicht

01
Einführung EU-DSGVO

Datenschutz

erste Schritte EU-DSGVO

Artikel 4

02
Vertiefung EU-DSGVO

Kapitel 1
Art. 1 - 3

Kapitel 2
Art. 5 – 7, 9

Kapitel 3
Art. 12 - 23

Kapitel 4
Art. 25 - 32

03
Grundlagen Sicherheit

Schutzziele

BSI

Grundschutz

Standards

ISMS

ISO 27x

ISIS 12 für KMU

04
Angriff Abwehr

Angriffsvarianten

Layer 8 Problem

Angriffsvorbereitung

Schadsoftware

Sicherheitssoftware

05
Angriff Abwehr

Angriffe auf Serverdienste

Brute Force

DoS & DDoS

Flooding

Tools

Agenda

- 01 Angriffsvarianten
- 02 Angriffsvorbereitung
- 03 Layer 8 Problem
- 04 Spyware, Phishing, Browser Highjacking
- 05 Schadsoftware
- 06 Sicherheitssoftware

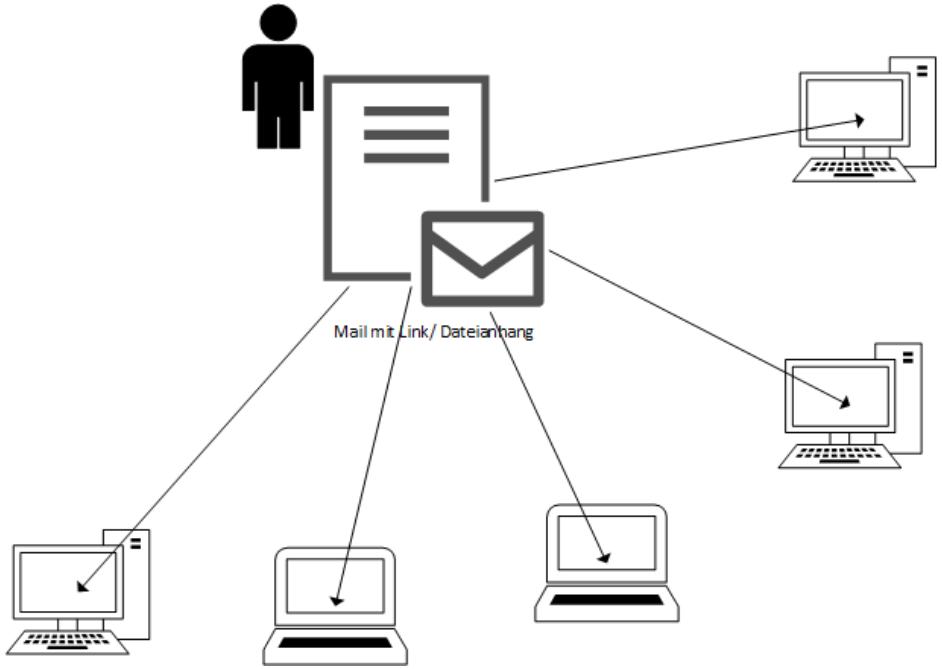
01 Angriffsvarianten

- *Massenangriff*
- *Gezielte Angriffe*

02 Massenangriff

Kein direktes Ziel definiert, Maximalprinzip: definierter Einsatz mit größtmöglicher Wirkung

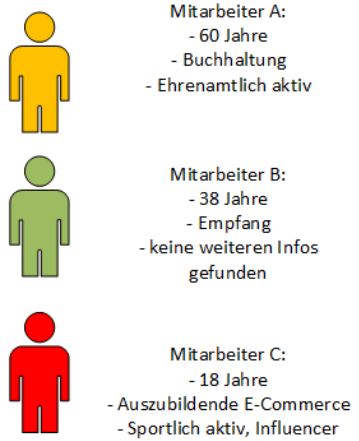
- Angreifer versendet Mails an eine möglichst große Zahl an Empfängern
- Text, Inhalt, Layout sind gleichbleibend
- Schadsoftware hängt an oder es ist ein Link enthalten



02 gezielter Angriff

Es wird gezielt ein Opfer ausgewählt und der Angriff angepasst

- Hoher Zeitaufwand
- Viel Recherchearbeit notwendig
  - z.B. über Facebook nach aktuellen Infos zum Unternehmen
  - Mitarbeitersuche
- Auswahl einer Attacke entsprechend der Recherche



02 Angriffsvorbereitung

02 Angriffsvorbereitung

- Netzwerkscans
- Wardriving
- Sozial Engineering

02 Angriffsvorbereitung

Massenangriff

- Zielbeispiele:
  - hinzufügen zu einem Botnet
  - Ausspionieren von Daten
  - Manipulation der Hardware
  - Identitätsdiebstall
  - Anzeigen von Werbung

- Recherche nach Schwachstellen
- Nutzen von Verhaltenswahrscheinlichkeiten
- Drive by Infektion durch Webseiten verdrängt Mail von der Spitzenposition

02 Angriffsvorbereitung

Gezielter Angriff

- Ziel
- Recherche
- Ereigniskette
- Sozial Engeneering - Der Mensch als leichteres Ziel als die Technik oder
- Das Layer 8 Problem

03 Layer 8 Problem

03 Layer 8 Problem

- Etwa 85 % aller erfolgreichen Cyberangriffe sind nur auf Grund der bewussten oder unbewussten Mitwirkung der User erfolgreich !
- Sorgloser Umgang
- Leichtfertige vergabe von Berechtigungen (z.B. Smartphone)
- Ignorieren von Richtlinien
- Unbedachte Preisgabe von persönlichen Informationen (FB, etc.)
- Bequemlichkeit vor Sicherheit
- Macht der Gewohnheit

03 Layer 8 Problem

Irrtümer des 21. Jahrhunderts

- Ich habe doch nichts zu verbergen
- Welche Daten will man bei mir schon holen

Mehr als 7.500 Unternehmen haben weltweit den Handel mit (theoretisch anonymisierten) personenbezogenen Daten als Kerngeschäft.

Auch Ihre . .

Der Umfang an pbD, welche auf legale Weise erfasst werden kann ist erschreckend

03 Layer 8 Problem

Smartphone

- Berechtigungsgruppen (Kamera, Mikrophone, SMS, etc.)
  es verbirgt sich mehr dahinter, schauen Sie nach

- Automatisches Update
  ungewollte Funktionen könnten hinzugefügt werden
  entzogene Berechtigungen werden wieder hergestellt

03 Layer 8 Problem

Passwort

- 123456, 123456789, 12345678, 1234567, password, 111111, 1234567890, 123123, 000000, abc123 (2019)
- Wie ist es besser?
- Richtlinien!

03 Layer 8 Problem

Bequemlichkeit & WLAN

- Nicht immer die beste Wahl
- Angriffsszenarien
  z.B. evil twin

03 Layer 8 Problem

Illusion Anonymität

- ISP weiß mehr als man glauben mag
- Deanonymisieren funktioniert leichter als man vermutet
  - Anonymisieren
  - Pseudonymisieren
- KI‘s denken schneller als man sich vorstellen kann

03 Layer 8 Problem

Das alles und noch viel mehr führt zu dem Fazit,

Menschen sind leichter zu hacken als Maschinen

04 Spyware, Phishing, Browser Highjacking

04 Spyware, Phishing, Browser Highjacking

- Der Mensch als Ziel, der Mensch als Schwachpunkt. Wissen ist Macht und je mehr ich über einen Menschen weiß, desto höher ist die Wahrscheinlichkeit, dass er durch mich manipulierbar ist.
- Zahlreiche Schadsoftware unterstützt bei der Informationsbeschaffung. Sowohl bei Massenangriffen, als auch bei gezielten Angriffen.

04 Spyware, Phishing, Browser Highjacking

Spyware

- Spyware sind Programme, die darauf spezialisiert sind Informationen über den PC-Nutzer auszuspionieren.
- Persönliche Daten, Surfgewohnheiten, Vorlieben und Zugangsdaten sind einige Beispiele der Informationen, auf die es Spyware abgesehen hat.

04 Spyware, Phishing, Browser Highjacking

Phishing

- Mails, mit denen Cyber-Kriminelle nach Passwörtern und anderen persönlichen Informationen „fischen“.
- Häufig werden solche Mails wie die Mails von Geldinstituten, Paypal, Amazon oder ähnliches gestaltet um die Opfer zu täuschen. Empfänger werden aufgefordert ihre Zugangsdaten einzugeben (Beispiel)

04 Spyware, Phishing, Browser Highjacking

Keylogger

- Ein Keylogger dient dazu, Tastatureingaben eines Nutzers aufzuzeichnen.
- Kriminelle benutzen Keylogger, um persönliche Daten wie Passwörter direkt "von den Fingern" des Anwenders abzugreifen.

04 Spyware, Phishing, Browser Highjacking

Browser-Hijacker

- Browser-Hijacker sind kleine Programme, welche die Einstellungen des Browsers manipulieren, um Seitenaufrufe (etwa die Startseite) und Suchanfragen auf bestimmte Webseiten umzuleiten. Beispielsweise auf Phishingseiten.

05 Schadsoftware

- *Viren*
- *Würmer*
- *Trojaner*
- *PUA*
- *Adware*

05 Schadsoftware

Viren

- Ein Computervirus verbreitet sich von PC zu PC
- Er befällt Dateien oder Datenträger mit seinem Programmcode
- Ein Virus wird nur durch die „Hilfe“ eines Users (und Trigger) aktiv

05 Schadsoftware

Viren

- Ein Computervirus verbreitet sich von PC zu PC
- Er befällt Dateien oder Datenträger mit seinem Programmcode
- Ein Virus wird nur durch die „Hilfe“ eines Users (und Trigger) aktiv

05 Schadsoftware

Viren

- Datei- oder Link-Viren
  - Sie befallen ausführbare Programmdateien (z.B. .exe)
  - Fast alle Bestandteile von Windows und installierter Software sind davon betroffen
  - Sie schreiben ihre Codes in die jeweiligen Dateien
  - Wird die Anwendung gestartet, wird der Virus gegebenenfalls mit ausgeführt

05 Schadsoftware

Viren

- Makro-Viren
    - Sie verstecken sich nicht in Anwendungen, sondern in Word- und Excel-Dokumenten.
    - Beim Laden eines verseuchten Dokuments beginnt das Virus mit seiner Schadensroutine.
    - Diese können ein einfacher Scherz sein, aber auch ein schweren Schaden anrichten

05 Schadsoftware

Würmer

- Sie sind in der Lage sich selbständig innerhalb eines Netzwerks zu verbreiten, ohne Dateien direkt zu befallen und in der Regel ohne benötigten Nutzerzugriff.
- Oftmals als Mailanhang, einmal freigelassen vermehren sie sich im Netz, unter Umständen endlos und legt so Netzte lahm.
- Sie sind häufig auch mit Viren oder Trojanern im Gepäck unterwegs.

05 Schadsoftware

Trojaner

- Als Trojaner oder Trojanisches Pferd, werden scheinbar harmlose Programme bezeichnet, die weitere Schadsoftware versteckt mit sich führen, um diese auf den PC zu schleusen.

- Eine sehr gefährliche Form ist der Backdoor-Trojaner (RAT = Remote Access Trojaner), dieser führt Hilfsprogramme mit sich, die nach Aktivierung einen Fernzugriff auf den infizierten Computer ermöglichen.

05 Schadsoftware

Ransomware (ransom = Lösegeld)

- Ebenfalls der Familie der Trojaner zuzuordnen, gehört diese Schadsoftware zu einem stark anwachsendem Bereich der Cyberkriminalität. Sie findet sowohl bei Massenangriffen (z.B. Bundestrojaner), als auch bei gezielten Angriffen Anwendung. Bei gezielten Angriffen werden idR. die gesamten Systeme durch eine solche Schadsoftware verschlüsselt. Häufig wissen die Angreifer durch umfangreiche Recherche sehr genau, wie kostenintensiv eine Wiederherstellung der Systeme durch Backups ist und bieten entsprechende Schlüssel deutlich günstiger zu kauf an.

05 Schadsoftware

PUA und Adware sind häufig eher lästig als bedrohlich

- PUA (potentiell unerwünschte Anwendung) oder PUP (potentiell unerwünschtes Programm) stellen in der Regel keine direkte Gefahr für ein System dar. Eines der bekanntesten Beispiele ist eine Toolbar, die sich direkt mit einer heruntergeladenen Anwendung installiert.
- Nichts desto trotz verbergen sich hinter solchen Anwendungen fleißige Datensammler und eine umgehende Deinstallation sollte erfolgen

05 Schadsoftware

PUA und Adware sind häufig eher lästig als bedrohlich

- Adware ist den meisten bekannt durch die Nutzung „kostenloser“ Apps.
- Zusätzlich zur eigentlichen Anwendung wird Werbung angezeigt oder ein zusätzliches Programm installiert welches Werbung anzeigt.
- Häufig ist die „kostenlose“ Software nur mit der entsprechenden Adware nutzbar.
- Erwirbt man eine Lizenz für die Anwendung, wird die Adware deinstalliert.
- Es hat halt alles seinen Preis . . .

06 Sicherheitssoftware

06 Sicherheitssoftware

Cybersecurity – Software

- Schon lange weit mehr als „nur“ Antivirus . . .
- Anti Virus, Anti Malware, Anti . . . weicht KI gestützter Endpointsecurity
- Zukunftsweisend sind jedoch Ansätze, die noch weit darüber hinaus gehen
- Sicherheitskonzepte alleine auf der Ebene von Geräten oder Anwendungen haben ausgedient und werden zukünftig lediglich Bestandteil eines ISMS sein

6 Antivirenprogramme

Antivirenprogramme waren gestern !

- **Überwachung von Sicherheitsstatus und Bedrohungen**
  Firewall und Sicherheitssoftware auf den Hosts arbeiten zusammen und tauschen kontinuierlich Sicherheitsinformationen aus. So kennen Sie immer den Sicherheitsstatus Ihres Netzwerks und werden im Falle aktiver Bedrohungen sofort benachrichtigt
- **Automatische Isolierung von Bedrohungen**
  Wird eine Bedrohung entdeckt, ergreifen beide gemeinsam automatische Reaktionsmaßnahmen mit dynamischen Firewall-Regeln und Lateral Movement Protection. Kompromittierte Hosts werden isoliert, um eine Ausbreitung, Hacker-Kommunikation und Datenverluste zu verhindern.

6 Antivirenprogramme

Sicherheitssoftware

- Deep learning KI aus der Security nicht mehr wegzudenken
  - Anwendungsanalyse
  - Punktgenaue Isolation von Bedrohungen
  - Nicht betroffene Teile des Netzwerks bleiben arbeitsfähig
  - Hochkomplexe Kombinationen und Kooperationen

6 Antivirenprogramme

Sicherheitssoftware

- Techniken von Virenscannern:
  - Reaktiv: Bei dieser Art der Erkennung wird ein Schädling erst erkannt, wenn eine entsprechende Signatur (oder bekannter Hash-Wert in der Cloud) seitens des Herstellers der Antivirensoftware zur Verfügung gestellt wurde.
    - Vorteil: Eine Signatur kann innerhalb kurzer Zeit erstellt werden und bildet daher immer noch das Rückgrat eines jeden Scanners (bei Onlineverbindungen zusätzlich Cloud-basierte Erkennung)
    - Nachteil: Ohne aktualisierte Signaturen werden keine neuen Schadprogramme erkannt.

6 Antivirenprogramme

Sicherheitssoftware

- Techniken von Virenscannern:
  - Proaktiv: Dies bezeichnet die Erkennung von Malware, ohne dass eine entsprechende Signatur zur Verfügung steht. Aufgrund der rapiden Zunahme neuer Schadprogramme werden solche Techniken immer wichtiger. Proaktive Verfahren sind etwa die Heuristik, Verhaltensanalyse oder die SandBox-Techniken.
    - Vorteil: Erkennung noch unbekannter Schadprogramme.
    - Nachteil: Die komplexe Technik bedarf hoher Entwicklungskosten und langer Entwicklungszyklen. Proaktive Techniken haben Prinzip bedingt gegenüber reaktiven eine höhere Fehlalarmquote. Aber besser einmal zu viel, als einmal zu wenig.

VIELEN DANK!

Quellen

- Grafiken:
- https://storyset.com