Schutzkonzepte gegen Malware entwickeln

Fach	IT-Technik
Lernfeld	LF 4: Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen
Querverweise zu weiteren Lernfeldern des Lehrplans	LF 1: Das Unternehmen und die eigene Rolle im Betrieb beschreiben LF 2: Arbeitsplätze nach Kundenwunsch ausstatten LF 3: Clients in Netzwerke einbinden LF 7: Cyber-physische Systeme ergänzen LF 11b, 11d, 11 (SE): Betrieb und Sicherheit vernetzter Systeme gewährleisten
Zeitrahmen	12 Unterrichtstunden
Benötigtes Material	Beamer und Dokumentenkamera, Rechner für je zwei Schüler/innen mit Office-Software, Informationsblätter, zentrale Dateiablage, Übungs-Rechner oder -Laptops

Kompetenzerwartungen

Die Schülerinnen und Schüler …

- lernen die Schutzziele der Informationssicherheit kennen und können diese nach definierten Kriterien beurteilen.
- analysieren Bedrohungen und Angriffe auf die Informationssicherheit und beurteilen Erfolgsaussichten von Angriffen auf IT-Systeme.
- stellen Schutzmaßnahmen zur Gewährleistung der Informationssicherheit dar.
- erklären, wie der Datenschutz funktioniert diese nach definierten Kriterien beurteilen.
- richten eine Datensicherung zum Schutz gegen Ransomware ein und bewerten diese.
- verschlüsseln Dateien und bewerten deren Nutzen.
- vollziehen die Wirkung von Office-Makros nach und bewerten deren Nutzen.

Aufgabe

1. **Orientieren:**

   Die Werbeagentur GAB GmbH wurde über einen gezielten Phishing-Angriff von der Malware Emotet befallen. Dadurch wurde auch Ransomware eingeschleust. Wichtige Firmendaten wurden durch Verschlüsselung unbrauchbar gemacht und es wurde ein Lösegeld für deren Entschlüsselung verlangt. Aus diesem Grund beauftragt die Firmenleitung der GAB GmbH die Firma JackSEC GmbH, sie zu beraten, wie in Zukunft Bedrohungen durch Malware reduziert und so weitere Schäden vermieden werden können.
   Die Schülerinnen und Schüler werden als Mitarbeiter der Firma JackSEC GmbH diesen Auftrag übernehmen. Sie werden die GAB beraten und sie bei der praktischen Umsetzung von Sicherheitsmaßnahmen unterstützen.

2. **Informieren:**

   Zum Einstieg sind die Begriffe Phishing, Malware, Ransomware und Emotet jeweils kurz zu erklären. Um weiter in das Thema Informationssicherheit einzusteigen, wird ein Senior Analyst der JackSEC GmbH (Lehrkraft) die Schülerinnen und Schüler mit einem Vortrag darüber informieren. Anschließend sind dazu in Teamarbeit mit Hilfe der Vortragsfolien und eines Infotextes zu den Grundlagen der Informationssicherheit die zu diesem Thema vorgegebenen Fragen zu beantworten. Die Teams sollen ihre Antworten auf die zur Verfügung gestellte Dateiablage hochladen. Der Senior Analyst sichtet die Antworten und bespricht sie mit den einzelnen Teams.

3. **Planen:**

   Um die Beratung der GAB GmbH besser planen zu können, müssen die Teams Kompetenzen zu Bedrohungen und Angriffen aufbauen. Dazu sollen in einem ersten Schritt angegebene Bedrohungen bzw. Angriffe den betroffenen Schutzzielen zugeordnet werden.
   Bei Emotet handelt es sich um einen zielgerichteten und äußerst gefährlichen APT-Angriff. Wie APT-Angriffe funktionieren und welche Schäden diese Angriffe anrichten können, sollen die Teams beispielhaft am Emotet-Angriff erklären. Dazu erstellen sie jeweils eine Präsentation oder ein Informationsblatt.

4. Durchführen:

Um die Informationssicherheit in Unternehmen zu schützen sind meist umfangreiche Schutz- und Abwehrmaßnahmen nötig. Deshalb beschäftigen sich die Schülerinnen und Schüler im nächsten Schritt selbstständig und eigenverantwortlich mit Bedrohungen und Angriffen auf die Informationssicherheit. Sie lernen so die wichtigsten organisatorischen bzw. technischen Maßnahmen kennen, die nötig sind, um im betrieblichen Umfeld die Informationssicherheit zu schützen.

In einem Gruppen-Puzzle erstellen die Experten-Gruppen Kurzpräsentationen und Quizze zu wesentlichen Themen der Informationssicherheit. Die Themenvorschläge und Informationen dazu werden aus einzelnen Videos aus der BSI-Mediathek entnommen. In den Stammgruppen stellt dann jeder Experte jeweils seine Kurzpräsentation am Gruppentisch vor. Am Ende jedes Vortrags wird dann auch das entsprechende Quiz durchgeführt. Im letzten Schritt lernen die Schülerinnen und Schüler die wesentlichen Aspekte des Datenschutzes in Partnerarbeit kennen und erstellen für eine firmenweite Awareness-Maßnahme Poster zu den goldenen Regeln der Informationssicherheit.

Im praktischen Teil richten die Teams eine Datensicherung ein und testen diese. Mit Hilfe von vorbereiteten Shell-Skripten können sie anschaulich lernen, wie Ransomware funktioniert. Das Erstellen eines Office-Makros hilft, zu verstehen, wie Office-Programme zum Einschleusen von Malware genutzt werden können. Leistungsfähige Schülerinnen und Schüler können optional tiefer in die Themen Datensicherung und Makro-Programmierung einsteigen.

5. Kontrollieren und Bewerten:

Am Ende diskutieren die Schülerinnen und Schüler in Gruppen über Aufgabenstellungen, Schwierigkeiten und Lösungs-Alternativen und geben Feedback. Über ein Formular können sie auch ihren eigenen Lernfortschritt beurteilen.

Hinweis zum Unterricht

Die Informationssicherheit ist ein sehr umfangreiches Themengebiet. Deshalb ist es nötig, dass den Schülerinnen und Schülern bereits am Anfang ihrer Ausbildung zumindest die wesentlichen Zusammenhänge zwischen den Bedrohungen der Informationssicherheit, den betroffenen Schutzzielen und den entsprechenden Schutzmaßnahmen anschaulich vermittelt und möglichst verständlich zugängig gemacht werden. Die zentrale Dateiablage hilft, die Arbeitsergebnisse zu sichern und so den Lernfortschritt der einzelnen Teams im Blick zu haben. Im Idealfall wird die Lernsituation komplett über einen entsprechenden Mebis-Kurs

bearbeitet.

Für die praktischen Übungen sind teilweise administrative Rechte nötig. Ideal sind Übungs-Rechner, die sich auch von den Schülerinnen und Schülern einfach am Ende der Praxisphase restaurieren lassen.

Querverweise zu anderen Fächern / Fachrichtungen

Grundlagenwissen zur Informationssicherheit wird praktisch in allen technischen Fächern/Lernfeldern der IT-Berufe benötigt. Nicht vergessen werden sollte, dass auch bei Cyber-physischen Systemen (LF 7) die IT-Sicherheit eine wesentliche Rolle spielt.

Quellen- und Literaturangaben

- Trojaner Emotet wieder aktiv: https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner-Emotet-greift-Unternehmensnetzwerke-an.html (Zugriff 03-09-2020. 12:05 MEZ)
- BSI - Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/
- BSI-Mediathek: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Mediathek/mediathek_node.html

Anhang

- Lernsituation
- Vortragsfolien

IT-Technik

Malware bei der GAB GmbH

Aufgabe

Die Werbeagentur GAB GmbH wurde von der Malware Emotet befallen. Durch diese Schadsoftware wurde auch Ransomware nachgeladen. Dies führte dazu, dass wichtige Dateien durch Verschlüsselung unbrauchbar gemacht wurden.
Die Firmenleitung der GAB beauftragt die Firma JackSEC GmbH, sie zu beraten, wie in Zukunft Bedrohungen durch Malware reduziert und so weitere Schäden vermieden werden können.

Ziele

- die Schutzziele der Informationssicherheit analysieren und einordnen
- Bedrohungen und Angriffe auf die Informationssicherheit kennenlernen
- Schutzmaßnahmen zur Gewährleistung der Informationssicherheit darstellen
- erklären, wie der Datenschutz funktioniert
- eine Datensicherung zum Schutz gegen Ransomware einrichten
- Dateien verschlüsseln
- Word-Makros kennenlernen

LS_01_Malware bei der GAB GmbH.doc

Arbeitsanleitung

Hinweis: Für die weitere Bearbeitung beachten Sie bitte die Hinweise zum Unterricht!

1 Ausgangssituation - Das Problem

Die Werbeagentur GAB GmbH wurde über einen gezielten Phishing-Angriff von der Malware Emotet befallen. Dadurch wurde auch Ransomware eingeschleust. Wichtige Firmendaten wurden durch Verschlüsselung unbrauchbar gemacht und es wurde ein Lösegeld für deren Entschlüsselung verlangt. Aus diesem Grund beauftragt die Firmenleitung der GAB die Firma JackSEC GmbH, sie zu beraten, wie in Zukunft Bedrohungen durch Malware reduziert und so weitere Schäden vermieden werden können.

Sie als MitarbeiterIn der Firma JackSEC GmbH werden zusammen mit Ihrem Team diesen Auftrag übernehmen. Sie werden die GAB beraten und sie bei der praktischen Umsetzung von Sicherheitsmaßnahmen unterstützen.

Aufgabe: Erklären Sie jeweils kurz, was Phishing, Malware, Ransomware und Emotet ist. **A**

2 Grundlagen der Informationssicherheit

A

Aufgabe: Ein Senior Analyst der JackSEC GmbH (Lehrkraft) wird Sie mit einem Vortrag zum Thema Informationssicherheit informieren.
Beantworten Sie anschließend mit Hilfe des Infotextes zu den Grundlagen der Informationssicherheit auf S.11 im Anhang und mit den Informationssicherheit-Vortragsfolien die nachfolgenden Fragen.
Einigen Sie sich in Ihrem Team jeweils auf eine Antwort. Laden Sie Ihre Antworten zusammen mit den Fragen auf die zur Verfügung gestellte Dateiablage hoch.
Der Senior Analyst bespricht anschließend die Antworten mit Ihnen.

1.) Was ist Informationssicherheit?

2.) Erläutern Sie die Schutzziele der Informationssicherheit und geben Sie jeweils eine typische Sicherheitsmaßnahme an.

3.) Was ist das *Recht auf informationelle Selbstbestimmung*?

4.) Was schützt der Datenschutz?

5.) Die Verfügbarkeit von IT-Systemen wird in Prozent angegeben. Fällt ein IT-System in 100 Tagen einen Tag lang aus, hat es eine Verfügbarkeit von 99%. Welche Verfügbarkeit ist nötig, wenn das IT-System in einem Jahr nur insgesamt 3,5h ausfallen darf?

6.) Welches Schutzziel ist der Grund, dass Server meistens 2 oder sogar 3 Netzteile haben?

7.) Nennen Sie 2 organisatorische und 2 technische Maßnahmen zur Gewährleistung der Informationssicherheit.

8.) Nennen Sie 5 konkrete Anwendungsfälle, bei denen zur Gewährleistung der Vertraulichkeit die verarbeiteten Daten verschlüsselt werden.

9.) Was wird unter *Security-Awareness* verstanden?

10.) Bei einer Schlüssellänge von 64 Bit sind 2^64 Schlüssel möglich. Ein Rechensystem kann 10^11 Schlüssel pro Sekunde erzeugen. Wie lange dauert das Erzeugen aller möglichen Schlüssel?

3 Bedrohungen und Angriffe auf die Informationssicherheit

Aufgabe: Ordnen Sie die angegebenen Bedrohungen bzw. Angriffe den betroffenen Schutzzielen zu (Mehrfachnennungen sind möglich). **A**

Bedrohung, Angriff	**betroffene Schutzziele**		
	Vertraulichkeit	**Integrität**	**Verfügbarkeit**
Beispiel: ein Sachbearbeiter hat absichtlich die Quartalszahlen gefälscht		***x***	
eine E-Mail wird von einem Hacker verändert an den Empfänger weitergeschickt			
eine Denial-of-Service Attacke			
eine Distributed-Denial-of-Service Attacke			
ein Angreifer liest Ihre E-Mail ohne dass Sie davon wissen			
Forschungsdaten wurden von Unbekannten verändert			
ein Trojaner verursacht einen Serverausfall			
durch Ransomware wurden Dateien verschlüsselt			
wegen einer defekten Festplatte steht die Fertigung still			
die VPN-Verbindung wurde gehackt			
der WLAN-Schlüssel wurde entwendet			
wegen einer Überschwemmung sind Datenträger unbrauchbar geworden			
Programme wurden durch Viren verändert			
ein Kollege hat Daten an Wetbewerber verkauft			
auf dem Mailserver läuft ein Fernsteuerungstrojaner			
Skript-Kiddies haben ein Krankenhaus angegriffen, auf Patientenakten konnte tagelang über das Internet zugegriffen werden			

Aufgabe: Wie funktioniert Emotet? **A**

Der Emotet-Angriff ist ein APT-Angriff. APT steht für *Advanced Persistent Threat* und bedeutet „fortgeschrittene andauernde Bedrohung“. APT-Angriffe sind zielgerichtet, äußerst gefährlich und richten große Schäden an. Sie werden meist von einem größeren Team von fortgeschrittenen, gut organisierten und professionell ausgestatteten Angreifern über längere Zeit mit enormem Aufwand vorbereitet. Einer der ersten APT-Angriffe fand 2010 mit Stuxnet statt und diente mutmaßlich dazu, das iranische Atomprogramm zu stören.

Hier wird beschrieben, wie der Emotet-Angriff funktioniert. Stellen Sie dies in einer Präsentation oder in einem Informationsblatt kurz dar.

Aufgabe: Was ist ein CEO-Fraud Angriff? **A**

Erklären Sie genau wie ein CEO-Fraud Angriff funktioniert und geben Sie an, was z.B. die Polizei zum Schutz davor rät.

4 Informationssicherheit schützen

Aufgabe: Ordnen Sie die Schutz- und Abwehrmaßnahmen den betroffenen Schutzzielen zu und geben Sie an, ob es sich um eine organisatorische oder technische Maßnahme handelt. (Mehrfachnennungen möglich) **A**

Schutz, Abwehrmaßnahme	organisatorisch	technisch	**Schutzziele**		
			Vertraulich-keit	**Integrität**	**Verfügbar-keit**
Beispiel: in einen Serverschrank wird eine USV eingebaut		***x***			***x***
bei einem VPN werden alle Daten verschlüsselt übertragen					
auf einem RAID-1 Plattensystem werden die Daten zuverlässiger gespeichert					
ein Dokument wird als "Verschlusssache" deklariert					
ein Dokument wird "nur zum internen Gebrauch" klassifiziert					
beim Backup werden Prüfsummenverfahren angewandt					
den Serverraum düfen nur Admins betreten					
seit heute werden verschlüsselte Backups angelegt					
am Eingang werden Personenkontrollen durchgeführt					
alle USB-Datenträger und Notebookfestplatten werden ab sofort verschlüsselt					
aller MitarbeiterInnen müssen an regelmäßigen Schulungen zur Informationssicherheit teilnehmen					
E-Mail-Anhänge von Unbekannten dürfen nicht geöffnet werden					
E-Mails werden vor dem Senden verschlüsselt					
die Türen der Serverschränke werden abgeschlossen					

Aufgabe: In der BSI-Mediathek befinden sich viele Videos zum Thema Informationssicherheit. Bilden Sie 5er Gruppen. Jeder Gruppe wird mit einem Buchstaben bezeichnet (A, B, ...). Innerhalb einer Gruppe werden an die Gruppenmitglieder die Zahlen 1 bis 5 vergeben. Wählen Sie in Ihrer Gruppe ein beliebiges Video aus und fassen Sie in der Gruppe die wichtigsten Aussagen des Videos zu einer Kurzpräsentation (max. 5 Min) zusammen. Jede Gruppe muss auch zu Ihrem Thema ein passendes kurzes Quiz vorbereiten (z.B. Karteikarten, Kahoot!, ...). **A**

Nach Ablauf der Bearbeitungszeit werden nach den vergebenen Zahlen neue Gruppen gebildet (alle 1er, alle 2er, ...). Innerhalb diesen Gruppen werden dann an den Gruppentischen abwechselnd die einzelnen Präsentationen gehalten. Nach jeder Präsentation nehmen die jeweiligen Zuhörer am Quiz teil.

5 Datenschutz

Aufgabe: Beantworten Sie mit Hilfe des Infotextes zum Datenschutz auf auf S.13 im Anhang und mit den Informationssicherheit-Vortragsfolien die folgenden Fragen. A
Einigen Sie sich in Ihrem Team jeweils auf eine Antwort. Laden Sie Ihre Antworten zusammen mit den Fragen auf die zur Verfügung gestellte Dateiablage hoch. Der Senior Analyst bespricht anschließend die Antworten mit Ihnen.

1.) Welches Persönlichkeitsrecht stellt die Grundlage des Datenschutzes dar?

2.) Erklären Sie an Beispielen zum Datenschutz, welche Daten personenbezogen sind und welche nicht.

3.) Erläutern Sie die folgenden Prinzipen des Datenschutzes: *Verbot mit Erlaubnisvorbehalt*, *Zweckbindung*, *Datensparsamkeit*.

4.) Welches DSGVO-Prinzip ist die gemeinsame Schnittmenge zwischen Datenschutz und IT-Sicherheit?

5.) Welche Aufgaben hat der betriebliche Datenschutzbeauftragte (DSB) gemäß Artikel 39 DSGVO?

6.) Fragen zu den Anforderungen an die Sicherheit der Datenverarbeitung (§ 64, BDSG):

a) Was ist die *Datenträgerkontrolle*?

b) In Absatz 2, Satz 2 in § 64, BDSG wird folgende Maßnahme beschrieben: "*.. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.*" Welche Schutzmaßnahme der IT-Sicherheit ist damit gemeint?

c) Welche Maßnahme steht hinter einer Zugangstür mit Iris-Scanner?

d) Erläutern Sie die Unterschiede zwischen *Zugangskontrolle* und *Zugriffskontrolle*.

7.) Warum kann Cloud-Computing datenschutzrechtlich höchst problematisch sein?

Aufgabe: Sie sollen die GAB GmbH im Rahmen ihrer firmenweiten Awareness-Maßnahme unterstützen. Dazu erstellen Sie in Ihrem 4er-Team ansprechende Poster zum Thema: "Die 12 goldenen Regeln zur Informationssicherheit am Arbeitsplatz". A
Ihr Senior Analyst (Lehrkraft) wird Ihnen zu Ihren Arbeitsergebnissen ein Feedback geben.

6 Praxis

6.1 Datensicherung und Versionierung mit FreeFileSync

A

Informieren

1.) Was ist eine Datensicherung?

2.) Geben Sie die 3 wesentlichen Aussagen der "3-2-1-Regel der Datensicherung" an!

3.) Was bedeutet *Versionierung*?

Datensicherung mit Versionierung bedeutet, dass sich im Ziel-Verzeichnis der Sicherung immer der aktuelle Stand aller Dateien befindet (Vollbackup). Alte Dateien im Ziel-Verzeichnis werden aber nicht gelöscht, sondern weiterhin aufbewahrt. Ein Zugriff auf alle Versionsstände der Dateien ist somit jederzeit möglich. FreeFileSync ist ein Open Source Backup- und Synchronisierungs-Tool, das auch eine Versionierung einfach möglich macht.

Ausführen und kontrollieren

4.) Installation und Konfiguration von FreeFileSync

- erstellen Sie folgende Verzeichnisse:
  C:\Bilder , **C:\Backup\Bilder** und **C:\Backup\alte_Versionen**
- installieren Sie FreeFileSync (https://freefilesync.org)
- konfigurieren Sie FreeFileSync mit den folgenden Einstellungen (siehe nächste Seite 8):
- Quell-Verzeichnis: **C:\Bilder**
- Ziel-Verzeichnis: **C:\Backup\Bilder**
- Ziel-Verzeichnis für die Vorgängerversionen: **C:\Backup\alte_Versionen\%date%-%time%**

5.) Test 1

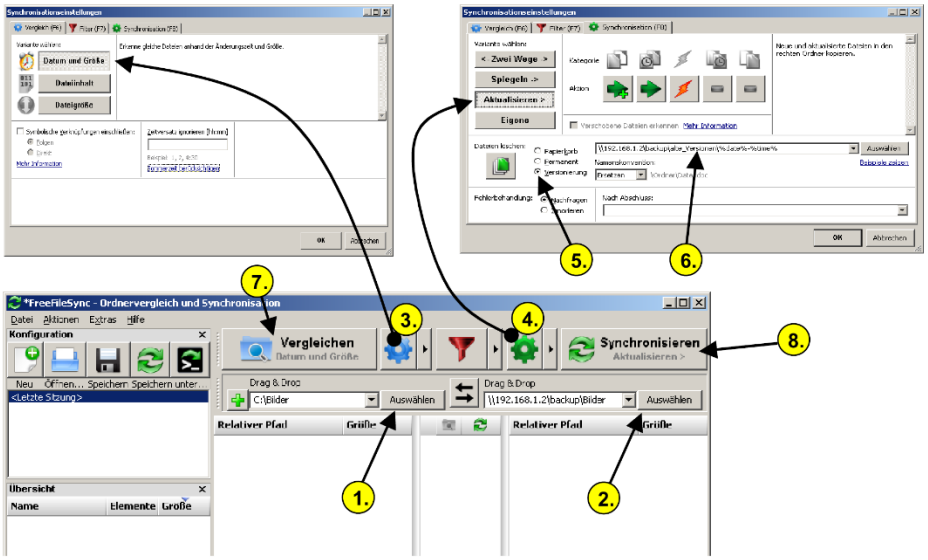
- kopieren Sie einige Dateien nach **C:\Bilder** und testen Sie dann die Synchronisierung
- ändern Sie einige der Dateien in **C:\Bilder** und synchronisieren Sie erneut und
- prüfen Sie nach, ob in **C:\Backup\alte_Versionen** ein Unterverzeichnis des entsprechenden Zeitstempels erzeugt wurde

6.) Test 2

- ändern Sie jetzt die Synchronisierungseinstellung von FreeFileSync auf *Spiegeln*
- löschen Sie alle Dateien in **C:\Bilder** und synchronisieren Sie erneut
- das Ziel-Verzeichnis ist nun leer
- Wo sind jetzt die Dateien, die sich vorher darin befanden?

7.) Um (z,B. verlorene) Dateien zurückzusichern, müssen Sie diese einfach aus dem Ziel-Verzeichnis der Sicherung herauskopieren. Probieren Sie das aus!

FreeFileSync konfigurieren



1. Verzeichnis, das gesichert werden soll (Quell-Verzeichnis) auswählen: **C:\Bilder**
2. Ziel-Verzeichnis auswählen: **C:\Backup\Bilder**
3. Vergleichen über das Zahnrad-Symbol auf "*Datum und Größe*" einstellen
4. Synchronisieren über das Zahnrad-Symbol auf "*Aktualisieren*" einstellen
5. in den Synchronisierungseinstellungen die Versionierung aktivieren und dort das
6. Ziel-Verzeichnis für die Vorgängerversionen auswählen:
   C:\Backup\alte_Versionen\%date%-%time%

Datensicherung (Synchronisierung) durchführen

7. Vergleich der beiden Verzeichnisse starten (und das Ergebnis überprüfen...)
8. Synchronisierung durchführen

nur für Profis: **Datensicherung mit FreeFileSync über die Kommandozeile** **P**

- speichern Sie die in FreeFileSync durchgeführten Einstellungen über *Datei --> Als Batchaufrag speichern* unter **C:\Backup\BatchRun.ffs_batch** ab
- testen Sie die Datensicherung durch Doppelklick auf den Batchauftrag oder auf einer Kommandozeile mit folgendem Befehl:
  `"C:\Program Files\FreeFileSync\FreeFileSync.exe" C:\Backup\BatchRun.ffs_batch`
- wenn alles funktioniert, können Sie den Batch-Auftrag so anpassen, dass sich der Fortschrittsdialog automatisch schließt und Fehler ignoriert werden
- verändern Sie in C:\Bilder einige Dateien und testen Sie alles noch einmal...

nur für absolute Profis: **Automatische Datensicherung mit FreeFileSync** **P+**

- öffnen Sie die Windows-Aufgabenplanung mit `taskschd.msc`
- erstellen Sie über *Aktion --> einfache Aufgabe erstellen* eine Aufgabe mit folgenden Einstellungen:
  Name: **Datensicherung**, *Trigger*: **beim Anmelden**, *Aktion*: **Programm starten**
  Programm starten: **"C:\Program Files\FreeFileSync\FreeFileSync.exe"**
  Argumente hinzufügen: **C:\Backup\BatchRun.ffs_batch**
- mit `schtasks /run /tn "Datensicherung"` kann die Aufgabe manuell auch sofort gestartet werden
- im Verzeichnis **%APPDATA%\FreeFileSync\Logs** können Sie die Logfiles aller Sicherungsläufe überprüfen
- jetzt alles testen, testen, testen...

6.2 Ransomware selbst gebaut - verschlüsseln und entschlüsseln mit 7-Zip

K

Informieren

1.) Ransomware verschlüsselt Dateien. Entschlüsseln ist nur mithilfe des entsprechenden Schlüssels möglich. Meistens muss für diesen Schlüssel ein Lösegeld bezahlt werden.
Ver- und Entschlüsselung ist mit vielen Programmen möglich, z.B. mit Packprogrammen. Wir verwenden die 7-Zip-Kommandozeilenversion 7z.exe aus den cmd-Tools.

2.) Probieren Sie Folgendes aus:

- öffnen Sie eine Eingabeaufforderung (Kommandozeile): **`cmd.exe`**
- erstellen Sie auf der Kommandozeile das Verzeichnis C:\Bilder: **`md C:\Bilder`**
- wechseln Sie in das Verzeichnis C:\Bilder: **`cd C:\Bilder`**
- erstellen Sie mit Notepad die Datei C:\Bilder\Test.txt: **`notepad C:\Bilder\Test.txt`**
  schreiben Sie einen beliebigen Text hinein und speichern Sie die Datei mit der Tastenkombination **`Strg-s`** ab und beenden Sie Notepad
- verschlüsseln Sie die Datei mit folgendem Kommando (der Schlüssel ist ***`Geheim`***):
  `7z.exe a -t7z -mhe -mx0 -sdel -p"Geheim" Test.txt.crypted Test.txt`
- öffnen Sie die verschlüsselte Datei Test.txt.crypted in Notepad:
  `notepad C:\Bilder\Test.txt.crypted`
  --> *jetzt ist die Datei-Inhalt ist völlig unlesbar!*
- entschlüsseln Sie die verschlüsselte Datei wieder
  `7z.exe e -aoa -p"Geheim" Test.txt.crypted`
- und öffnen Sie die entschlüsselte Datei anschließend wieder in Notepad
  --> *jetzt ist der Datei-Inhalt wieder lesbar!*

3.) Erstellen Sie mit notepad die beiden folgenden Batch-Dateien encrypt.cmd und decrypt.cmd oder laden Sie sie herunter.

```
:: encrypt.cmd - verschlüsselt alle Dateien im Verzeichnis
@echo off
set "key=qHF*@iDm2W~P!b2X9Df6iqAqy4Er?]"
for %%i in (*) do (
 if /i "%%~nxi" neq "encrypt.cmd" (
   7z.exe a -t7z -mhe -mx0 -sdel -p"%key%" "%%~fi.crypted" "%%~fi" >nul
   if errorlevel 0 echo encrypted: %%~fi
 )
)
pause
```

```
:: decrypt.cmd - entschlüsselt alle .crypted Dateien im Verzeichnis
@echo off
set "key=qHF*@iDm2W~P!b2X9Df6iqAqy4Er?]"
for %%i in (*.crypted) do (
 7z.exe e -aoa -p"%key%" "%%~fi" >nul
 if errorlevel 0 (
   echo decrypted: %%~fi
   del /F "%%~fi"
 )
)
pause
```

Ausführen und kontrollieren

4.) Jetzt können Sie einen Ransomware-Angriff simulieren, indem Sie

- wie beim Backup mit FreeFileSync im Verzeichnis C:\Bilder einige Dateien anlegen
- dann zuerst eine Datensicherung durchführen
- jetzt die Batch-Datei encrypt.cmd nach C:\Bilder kopieren und dort ausführen

im nächsten Schritt müssen Sie

entweder

- Lösegeld für die Entschlüsselung bezahlen
- dann bekommen Sie von den Hackern die Batch-Datei decrypt.cmd zugesandt
- diese müssen Sie nach C:\Bilder kopieren und dort ausführen

oder

- die Dateien einfach aus dem Backup Ziel-Verzeichnis C:\Backup\Bilder zurückholen

Probieren Sie beides aus!

6.3 Was sind eigentlich Makros?

A

Informieren

1.) Was sind eigentlich Word-Makros und wozu können Makros benutzt werden?

2.) Erläutern Sie, warum Word-Makros ein Sicherheitsrisiko für Ihren Computer darstellen können.

Planen, ausführen und kontrollieren

3.) Erstellen Sie ein Word-Makro, das für den aktuellen Text die durchschnittliche Satzlänge in Wörtern ermittelt und weisen Sie dem Makro die Tastenkombination `Strg-Alt-w` zu.

Die genauen Anleitungen finden Sie hier: - So schreiben Sie Word-Makros - einfach erklärt!
- Makro öffnen mit Tastenkombination

6.4 Ein gefährliches Word-Makro

P+

Informieren

1.) Informieren Sie sich in der c't 05/2017, S.142 über Word Makro-Viren: Analysiert: Das Comeback der Makro-Malware.

Planen, ausführen und kontrollieren

2.) Erstellen Sie jetzt einen Word Makro-Virus wie dies hier gezeigt wird.

6.5 Fazit und Erkenntnisse

A

Bewerten

1.) Diskutieren Sie in Ihrem Team, wie über Makros in Office-Programmen eingeschleuste Ransomware verhindert werden kann und wie der entstehende Schaden minimiert werden kann.

7 Anhang

7.1 Info-Text: Grundlagen der Informationssicherheit

Was ist Informationssicherheit? (nach de.wikipedia.org/wiki/IT-Sicherheit)

Die Informationssicherheit dient dem Schutz vor Gefahren und Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken bei IT-Systemen.
Sie umfasst neben der Sicherheit der in IT-Systemen gespeicherten Daten (IT-Sicherheit) auch die Sicherheit von nicht elektronisch verarbeiteten Informationen (z.B. auf Papier oder am Telefon).

Schutzziele der Informationssicherheit

Informationssicherheit ist das Gewährleisten der Schutzziele der Informationssicherheit!

Vertraulichkeit *confidentiality, privacy*	Schutz gegen den unbefugten Zugriff auf Daten, dies gilt sowohl bei gespeicherten Daten als auch während der Datenübertragung typische Sicherheitsmaßnahme: Verschlüsselung
Verfügbarkeit *availability*	Zuverlässigkeit und Funktionsfähigkeit von IT-Systemen, Verhinderung von Systemausfällen, der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden typische Sicherheitsmaßnahme: Redundanz
Integrität *integrity*	Unversehrtheit und Vollständigkeit der Daten, Schutz gegen die unbefugte (auch teilweise) Veränderung von Daten typische Sicherheitsmaßnahme: kryptografische Prüfsumme (Hash-Wert)
Authentizität *authenticity*	eindeutige Zuordnung einer Nachricht zu einem Sender wird vom BSI der *Integrität* zugerechnet, typische Sicherheitsmaßnahme: Passwort

IT-Sicherheit (Datensicherheit)

Die Informationssicherheit betrifft alle Verfahren und Systeme, auch nicht-technische. Die Informationssicherheit bei technischen Systemen wird IT-Sicherheit genannt (manchmal noch *Datensicherheit*).

Cyber-Sicherheit

Mit Cyber-Raum (Cyberspace) sind alle mit dem Internet verbundenen IT-Systeme und IT-Infrastrukturen (z.B. IoT-Systeme) gemeint. Wird die IT-Sicherheit von der kontrollierten Unternehmensumgebung auf den öffentlichen Cyber-Raum ausgeweitet, wird von Cyber-Sicherheit gesprochen.

Datenschutz

Der Datenschutz ist der Teil der Informationssicherheit, der gesetzlich geregelt ist und dem Schutz personenbezogener Daten dient bzw. die BürgerInnen vor der missbräuchlichen Verwendung ihrer Daten schützt.

Informationssicherheitsprozess

Das Informationssicherheits-Managementsystem (ISMS) ist die Planungs- und Lenkungsaufgabe, die erforderlich ist, um bei Firmen und Behörden einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen.

BSI IT-Grundschutz

Der IT-Grundschutz wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt. Er beschreibt eine Methode, wie Firmen und Behörden mit relativ geringem Aufwand und ohne Spezialisten-Wissen die Informationssicherheit schützen können. Das IT-Grundschutz-Kompendium erhält verständliche Anweisungen, wie mit geringem Aufwand ein angemessenes Sicherheitsniveau erreicht werden kann.

Bedrohungen und Angriffe auf die Informationssicherheit

- Katastrophen Feuer, Flut, Erdbeben ...
- Systemfehler Fehlfunktion, Absturz, Hardwaredefekt, Stromausfall ...
- interne Angriffe vorsätzliches Verändern oder Löschen von Daten, Ausspähen von Daten ...
- externe Angriffe Hacker, Malware, Phishing, APTs, ...

Maßnahmen zur Gewährleistung der Informationssicherheit

organisatorische Maßnahmen

- ISMS einführen + Informationssicherheitsbeauftragter (ISB)
- Datenschutzbeauftragter (DSB)
- Sensibilisierung und Schulung der MitarbeiterInnen (Awareness)
- IT-Notfallteam (CERT - Computer Emergency Response Team)

technische Maßnahmen

- Infrastruktur verschlossene Türen, Zutrittskontrolle, USV, Brandschutz, Alarmanlage, ...
- Netze redundante Wege, Segmentierung (VLAN), Firewall, sichere Zugänge mit VPN, ...
- IT-Systeme Malwareschutz, Datensicherung (Backup), Prüfsummen, Verschlüsselung, Update- und Patchmanagement, Systeme überwachen (Monitoring), ...
- Dienste Zugang nur mit Benutzerkennung und Passwort, Protokollierung, Berechtigungskonzept mit Zugriffsbeschränkungen, Plausibilitätsüberprüfung, ...

Verschlüsselung

Verschlüsselung gewährleistet Vertraulichkeit und **wird häufig eingesetzt**: z.B. bei der Übertragung von Webseiten (HTTPS) und E-Mails, bei der Administration entfernter Systeme (SSH), bei WLAN und VPN. Oft werden auch USB-Datenträgern und (Notebooks-)Festplatten verschlüsselt.

Beim **Verschlüsseln** werden die zu übertragenden Daten mit einem Verschlüsselungsverfahren und einem Schlüssel in eine für Andere unlesbare Form umgerechnet. Durch **Entschlüsseln** werden die Daten wieder lesbar.

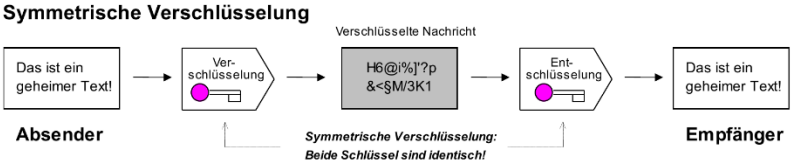
Symmetrische Verfahren (z.B. AES) verwenden für beide Vorgänge denselben Schlüssel.

Werden 2 unterschiedliche Schlüssel verwendet, z.B. ein öffentlicher und ein privater Schlüssel, handelt es sich um ein asymmetrisches Verfahren (Public-/Private-Key Verfahren, z.B. RSA).

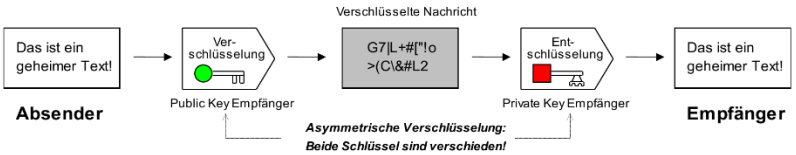
Beide Verfahren haben ihre Berechtigung, da bei symmetrischer Verschlüsselung der Schlüsselaustausch zwischen den Kommunikations-Partnern problematisch ist und asymmetrische Verfahren einen hohen Rechenaufwand verursachen. Aus diesem Grund werden meist beide Verfahren kombiniert: Hybride Verschlüsselung (z.B. bei TLS).

Kryptografische Prüfsummen (Einwegverschlüsselung, Hash-Verfahren) werden zur Integritäts-Prüfung eingesetzt (z.B. SHA256).

Symmetrische Verschlüsselung



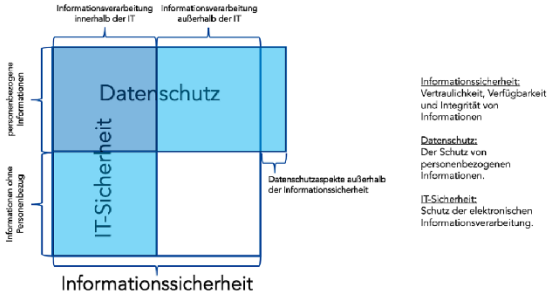
Asymmetrische Verschlüsselung (Public-/Private Key-Verfahren)



7.2 Info-Text: Datenschutz

Datenschutz

Der Datenschutz ist der Teil der Informationssicherheit, der gesetzlich geregelt ist und dem Schutz personenbezogener Daten dient bzw. die BürgerInnen vor der missbräuchlichen Verwendung ihrer Daten schützt.
Grundlage des Datenschutzes ist das *Recht auf informationelle Selbstbestimmung*, das jedem Einzelnen zusichert, über die Erhebung, Speicherung, Verwendung und Weitergabe der über ihn gespeicherten Daten selbst zu bestimmen.



Zusammenhang zwischen Informationssicherheit, IT-Sicherheit und Datenschutz

Die wichtigsten gesetzlichen Regelungen zum Datenschutz sind die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) und die Länderdatenschutzgesetze.

Personenbezogene Daten (Artikel 4, DSGVO)

Personenbezogene Daten sind es dann, wenn die Information einer bestimmten lebenden Person zugeordnet werden kann, z.B.: Telefonnummer, E-Mail Adresse, Kontonummer, Bild einer Person, KFZ-Kennzeichen, IP-Adresse (*Online-Kennung*), Positionsdaten (*Standortdaten*), Unterschrift, Kaufverhalten, Zeugnisse.

Mit welchen Prinzipien schützt die DSGVO den Datenschutz?

Verbot mit Erlaubnisvorbehalt	Verarbeitung nur, wenn es durch ein Gesetz erlaubt ist oder der Betroffene einwilligt
Zweckbindung	der vorher festgelegte Verarbeitungszweck darf später nicht verändert werden
Transparenz	Verarbeitung muss nachvollziehbar sein, Informationspflichten zu Zweck und Umfang
Datensparsamkeit	Datenmenge muss dem Zweck angemessen und auf das notwendige Maß beschränkt sein
Sicherheit der Verarbeitung	Vertraulichkeit, Integrität, Verfügbarkeit sicherstellen durch *technische und organisatorische Maßnahmen* (TOM), weitere Anforderungen an die Sicherheit der Datenverarbeitung finden sich in §64 BDSG

Datenschutzkontrolle

durch Datenschutzbeauftragte, z.B. der Bundesbeauftragte, die Landesbeauftragten für den Datenschutz und der betriebliche Datenschutzbeauftragte (DSB, Artikel 39 DSGVO).

Die Aufgaben des Datenschutzbeauftragten sind:
- Unterrichtung und Beratung
- Zusammenarbeit mit der Aufsichtsbehörde
- Überwachung der Datenverarbeitung
- Anlaufstelle für die Aufsichtsbehörde

8 Feedback

Mit diesem Bogen können Sie Ihren eigenen Lernfortschritt beurteilen.
Bitte machen Sie 1 Kreuz pro Zeile!

A

	30%	70%	100%	120%
Wieviele theoretische Aufgaben haben Sie bearbeitet? Schätzung!				
Wieviele praktische Aufgaben haben Sie bearbeitet? Schätzung!				

ich stimme	gar nicht zu	eher nicht zu	zu	völlig zu
Hat der Unterricht Ihre Selbstständigkeit gefördert?				
Ich war gefordert, selbstständig Informationen zu beschaffen und auszuwerten.				
Ich war gefordert, eigene Entscheidungen zu treffen.				
Ich habe Lösungsmöglichkeiten entwickelt und in praktisches Handeln umgesetzt.				
Hat der Unterricht Ihre Teamfähigkeit gestärkt?				
Ich war gefordert, partnerschaftlich mit anderen zusammenzuarbeiten.				
Ich musste auch mal unangenehme Arbeiten übernehmen.				
Ich war gefordert, Vereinbarungen einzuhalten.				
Hat der Unterricht die Kommunikationsfähigkeit gefördert?				
Ich war gefordert, schwierige Sachverhalte angemessen und klar darzustellen.				
Ich musste mich mit unterschiedlichen Meinungen auseinandersetzen.				
Ich war gefordert, Kritik konstruktiv zu formulieren.				
Hat der Unterricht die Methodenkompetenz gefördert?				
Ich war gefordert, Ergebnisse zu strukturieren und zu präsentieren.				
Ich musste schwierige Problemstellungen in einzelne zur Lösung notwendige Arbeitsschritte zerlegen.				
Hat der Unterricht Ihr Verantwortungsbewusstsein gefördert?				
Ich musste mich an gemeinsame Vereinbarungen halten.				
Ich war gefordert, die übernommenen Aufgaben zuverlässig zu erledigen und zu Ende zu führen.				
Hat der Unterricht Ihr Wissen erweitert?				
Ich bin mit den theoretischen Aufgaben gut zurecht gekommen.				
Ich bin mit den praktischen Aufgaben gut zurecht gekommen.				

nach: http://bk-suedstadt.de/fileadmin/dateien/01_Bildungsgaenge/02_Berufsschule/05_EH/eva_ls_schueler.htm

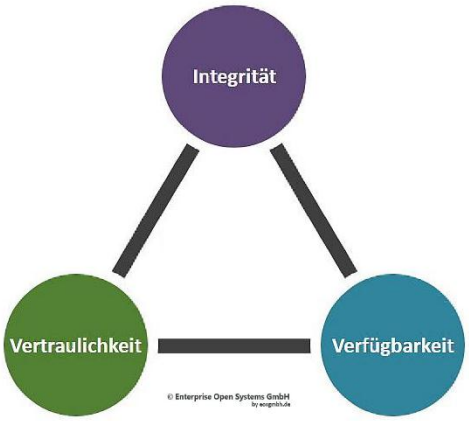
9 Fragen

- die folgenden Fragen stammen aus dem Fragenpool. Sie zeigen den Umfang und die Intensität der Unterrichtsinhalte und dienen zur Vorbereitung auf Leistungskontrollen und Abschlussprüfung
- *manchmal* haben schwierige Fragen ein Sternchen "*", schwierigere zwei "**"
- es werden KEINE Lösungen bereitgestellt, Ziel ist es, dass SIE die Lösungen selbst erstellen!
- Nachfragen, Anmerkungen, Lob und Kritik können Sie an Ihre Lehrkraft richten

1.) Was ist Informationssicherheit?
2.) Erläutern Sie folgende Begriffe: Phishing, Malware, Ransomware.
3.) Erläutern Sie die Schutzziele der Informationssicherheit und geben Sie jeweils eine typische Sicherheitsmaßnahme an.
4.) Was ist das Recht auf informationelle Selbstbestimmung?
5.) Was schützt der Datenschutz?
6.) Erläutern Sie die folgenden Prinzipien der DSGVO: Verbot mit Erlaubnisvorbehalt, Zweckbindung, Datensparsamkeit.
7.) Welches DSGVO-Prinzip ist die gemeinsame Schnittmenge zwischen Datenschutz und IT-Sicherheit?
8.) Bei der Verfügbarkeit wird als typische Sicherheitsmaßnahme Redundanz angegeben. Erklären Sie Redundanz an mehreren Beispielen.
9.) Die Verfügbarkeit von IT-Systemen wird in Prozent angegeben. Fällt ein IT-System in 100 Tagen einen Tag lang aus, hat es eine Verfügbarkeit von 99%. Welche Verfügbarkeit ist nötig, wenn das IT-System in einem Jahr nur insgesamt 3,5h ausfallen darf?
10.) Welches Schutzziel ist der Grund, dass Server meistens 2 oder sogar 3 Netzteile haben?
11.) Nennen Sie 2 organisatorische und 2 technische Maßnahmen zur Gewährleistung der Informationssicherheit.
12.) Nennen Sie 3 Anwendungsfälle, bei denen zur Gewährleistung der Vertraulichkeit die verarbeiteten Daten verschlüsselt werden.
13.) Was wird unter Security-Awareness verstanden?
14.) Bei einer Schlüssellänge von 64 Bit sind 2^64 Schlüssel möglich. Ein Rechensystem kann 10^11 Schlüssel pro Sekunde erzeugen. Wie lange dauert das Erzeugen aller möglichen Schlüssel?
15.) Nennen Sie 5 Anwendungsfälle bei denen die Informationssicherheit bedroht ist. Geben Sie jeweils auch die betroffenen Schutzziele an.
16.) Der Emotet-Angriff ist ein sogenannter APT-Angriff. Was ist ein APT-Angriff?
17.) Erläutern Sie, warum Word-Makros ein Sicherheitsrisiko für Ihren Computer darstellen können.
18.) Geben sie den wesentlichsten Unterschied zwischen symmetrischer Verschlüsselung und asymmetrischer Verschlüsselung an.
19.) Nennen Sie jeweils ein Problem der symmetrischen und der asymmetrischen Verschlüsselung.
20.) Wozu werden Hash-Verfahren eingesetzt?
21.) Was haben die folgenden Begriffe mit Verschlüsselung zu tun: SHA, RSA, AES?
22.) Nennen Sie 5 konkrete Anwendungsfälle, bei denen zur Gewährleistung der Vertraulichkeit die verarbeiteten Daten verschlüsselt werden
23.) Was ist eine Datensicherung?
24.) Geben Sie die 3 wesentlichen Aussagen der "3-2-1-Regel der Datensicherung" an!

Grundlagen der

Informationssicherheit



Agenda

- Was ist Informationssicherheit?
- Schutzziele
- Informationssicherheitsprozess
- Bedrohungen
- Maßnahmen
- Beispiele
- Datenschutz

  Verschlüsselung, 7-Zip, Goldene Regeln

Wo 12.07.2020

Was ist Informationssicherheit?

⇒ Informationssicherheit soll
- vor Gefahren und Bedrohungen schützen
- wirtschaftliche Schäden vermeiden
- Risiken minimieren

⇒ meint die Eigenschaften von IT-Systemen,
welche die folgenden Schutzziele gewährleisten:
- Vertraulichkeit
- Verfügbarkeit
- Integrität
- Authentizität

Schutzziele der Informationssicherheit

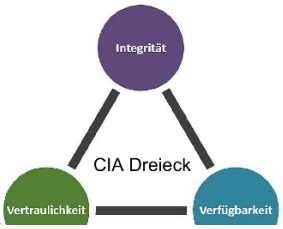
Informationssicherheit ist das *Gewährleisten* der **Schutzziele der Informationssicherheit!**

Vertraulichkeit
confidentiality, privacy
Schutz gegen den unbefugten Zugriff auf Daten
typische Sicherheitsmaßnahme: Verschlüsselung

Verfügbarkeit
availability
Zuverlässigkeit und Funktionsfähigkeit von IT-Systemen, Verhinderung von Systemausfällen
typische Sicherheitsmaßnahme: Redundanz

Integrität
integrity
Unversehrtheit und Vollständigkeit der Daten, Schutz gegen die unbefugte Veränderung von Daten
typische Sicherheitsmaßnahme: kryptografische Prüfsumme (Hash-Wert)

Authentizität
authenticity
eindeutige und nachweisbare Zuordnung einer Nachricht zu einem Sender
(die Authentizität wird vom BSI der Integrität zugerechnet)
typische Sicherheitsmaßnahme: Passwort



Begriffe

⇒ *Informationssicherheit* - betrifft alle Systeme, auch nicht-technische

⇒ *IT-Sicherheit* - betrifft technische IT-Systeme

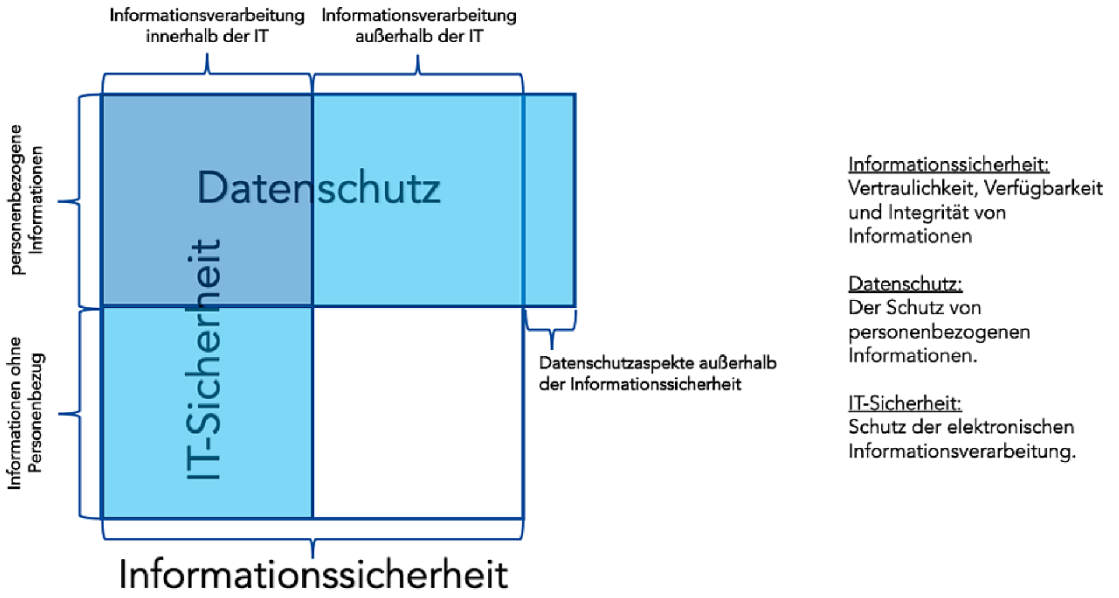
⇒ *Datensicherheit* - Synonym für *IT-Sicherheit* (*safety, security*)

⇒ *Datenschutz* - Schutz personenbezogener Daten (*privacy*)

⇒ *Cyber-Raum, Cyberspace*
alle mit dem Internet verbundenen IT-Systeme und IT-Infrastrukturen (z.B. IoT-Systeme)

⇒ *Cyber-Sicherheit*
IT-Sicherheit von der kontrollierten Unternehmens-umgebung auf den öffentlichen Cyber-Raum (Internet) ausgeweitet

Informationssicherheit, IT-Sicherheit, Datenschutz



Informationssicherheitsprozess

⇒ Planungs- und Lenkungsaufgabe (*Chefsache*)

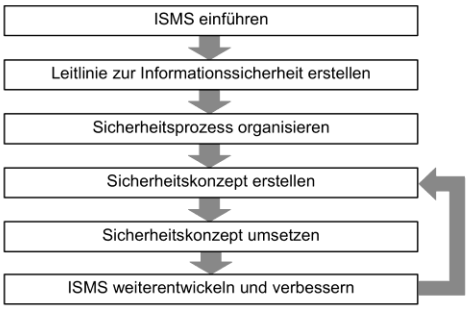
⇒ Prozess zur Herstellung von Informationssicherheit aufbauen und kontinuierlich umsetzen

⇒ wird als Informationssicherheits-Management bezeichnet

⇒ ISMS (*Information Security Management System*) einführen

⇒ Standards: ISO 27001 und BSI-Standard 200-1

⇒ IT-Sicherheit ist kein Zustand sondern ein Prozess!



Bedrohungen der Informationssicherheit

⇒ Katastrophen — Feuer, Flut, Erdbeben ...

⇒ Systemfehler — Fehlfunktion, Absturz, Hardwaredefekt, Stromausfall ...

⇒ interne Angriffe — vorsätzliches Verändern oder Löschen von Daten, Ausspähen von Daten ...

⇒ externe Angriffe — Hacker, Malware, Phishing, APT ...

⇒ das sind laut BSI: Elementare Gefährdungen

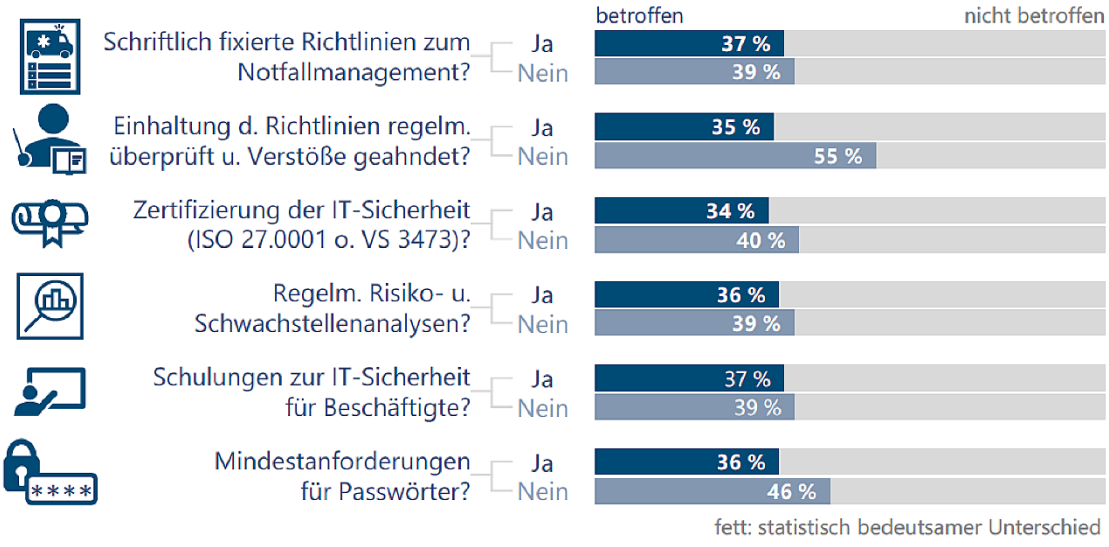
Maßnahmen zur Gewährleistung der Informationssicherheit

⇒ organisatorische Maßnahmen
- ISMS + Informationssicherheitsbeauftragter (ISB)
- Datenschutzbeauftragter (DSB)
- Sensibilisierung und Schulung der MitarbeiterInnen (*Awareness*)
- IT-Notfallteam (CERT - *Computer Emergency Response Team*)

⇒ technische Maßnahmen
- **Infrastruktur** verschlossene Türen, Zutrittskontrolle, USV, Brandschutz, Alarmanlage ...
- **Netze** redundante Wege, Segmentierung (VLAN), Firewall, VPN ...
- **IT-Systeme** Malwareschutz, Datensicherung, Prüfsummen, Verschlüsselung, Update- und Patchmanagement, Monitoring, IDS/IPS ...
- **Dienste** Zugang nur mit Benutzerkennung und Passwort, Protokollierung, Berechtigungskonzept (Zugriffsbeschränkungen), Plausibilitätsüberprüfung, ...

Grundlagen der Informationssicherheit Folie 8

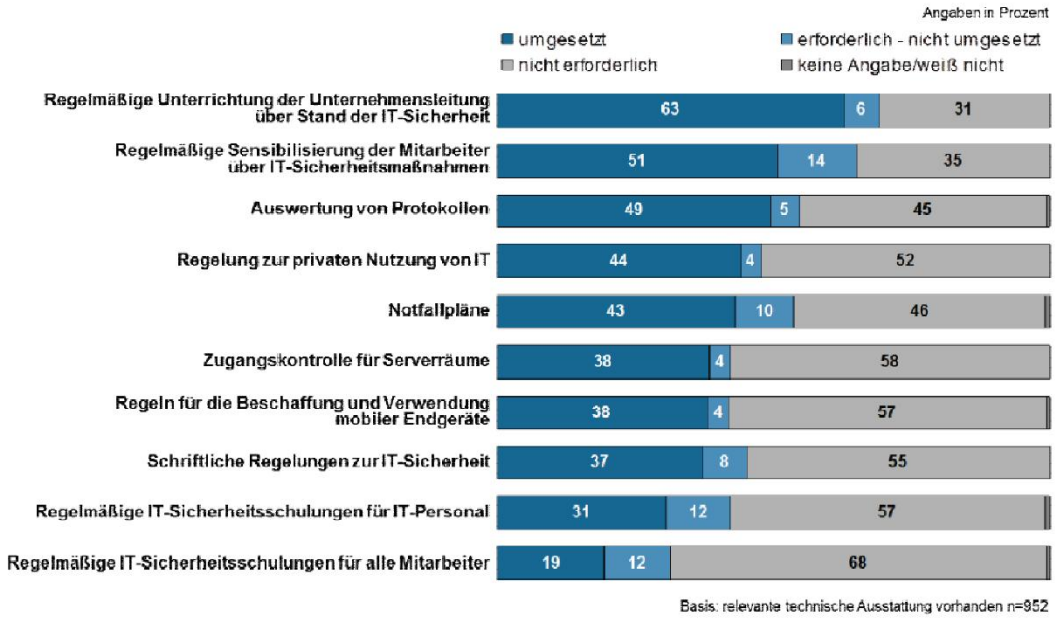
Anteile von Cyberangriffen betroffener Unternehmen nach IT-Sicherheitsmaßnahmen



https://kfn.de/blog/2020/03/neuer-forschungsbericht-veroeffentlicht-cyberangriffe-gegen-unternehmen-in-deutschland/

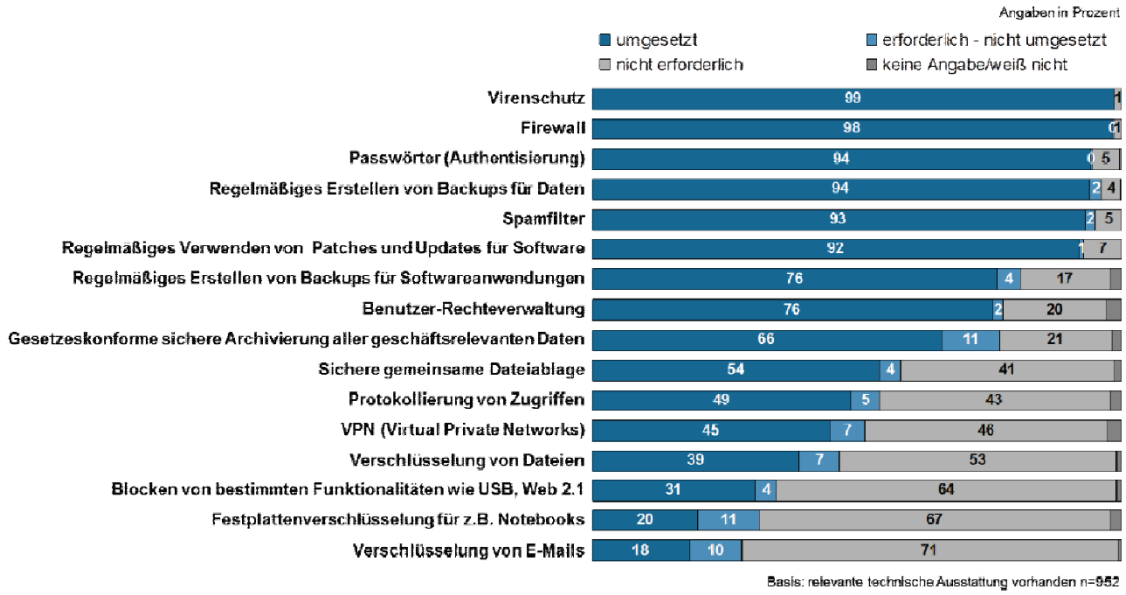
Grundlagen der Informationssicherheit Folie 9

Beispiel: Organisatorische Maßnahmen



Quelle: WIK-Consult Studie IT-Sicherheitsniveau in KMU 2011/12

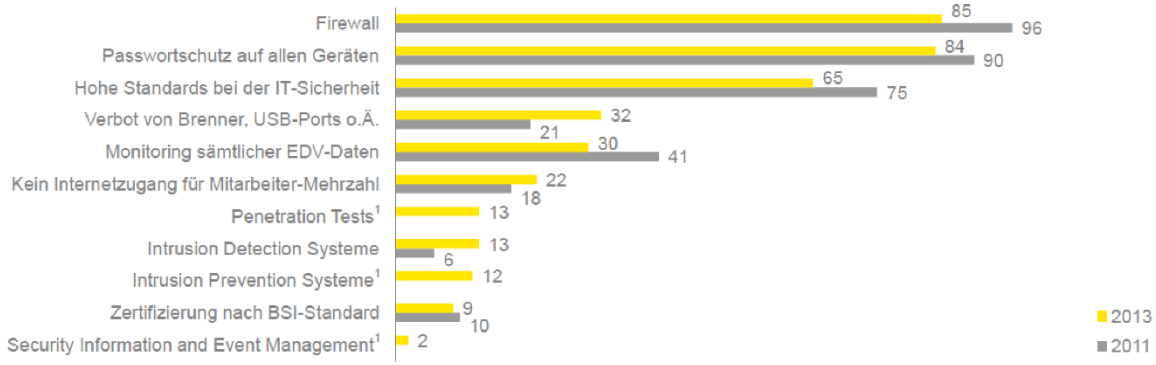
Beispiel: Technische Maßnahmen



Quelle: WIK-Consult Studie IT-Sicherheitsniveau in KMU 2011/12

Maßnahmen: *Blindes Vertrauen auf die Firewall*

Welche Sicherheitsvorkehrungen gegen Datenklau haben Sie im **IT-Bereich** getroffen?

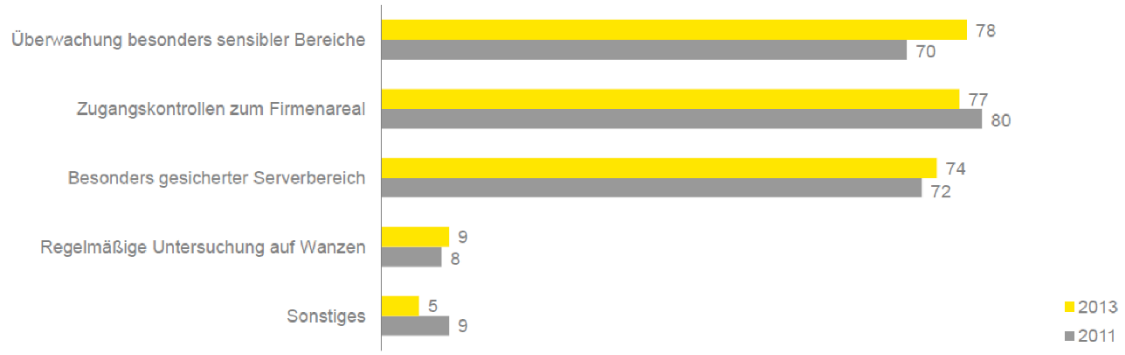


- mehr als 80 Prozent der befragten Unternehmen setzen zur Vorbeugung von Spionageakten auf Firewalls und Passwörter
- umfassendere Schutzvorkehrungen wie Penetration Tests oder das Intrusion Prevention System werden nur relativ selten benutzt

aus: http://www.ey.com/Publication/vwLUAssets/Praesentation_-_Datenklau_2013/%24FILE/EY-Datenklau-2013.pdf

Maßnahmen: Objektsicherheit

Welche Sicherheitsvorkehrungen Datenklau haben Sie im Bereich **Objektsicherheit** getroffen?



- die Sicherheitsvorkehrungen wurden seit 2011 nicht sonderlich aufgestockt
- der Anteil der Unternehmen, die sensible Unternehmensbereiche gesondert schützen, ist in etwa gleich geblieben

aus: http://www.ey.com/Publication/vwLUAssets/Praesentation_-_Datenklau_2013/%24FILE/EY-Datenklau-2013.pdf

Verschlüsselung

⇒ **Ziel:** Vertraulichkeit gewährleisten

⇒ Verschlüsselungs-Möglichkeiten

- symmetrische V. ein Schlüssel für Ver- und Entschlüsselung, AES
- asymmetrische V. Public/Private-Key-Verfahren, zwei Schlüssel: einer für Ver- und einer zur Entschlüsselung, RSA
- hybride V. Kombination von asymmetrischer und symmetrischer V., TLS
- Hash-Verfahren kryptografische Prufsumme, *Einwegverschlüsselung*, SHA

⇒ Schlüssellängen

- symmetrische V.: 128 - 256 Bit
- asymmetrische V.: 1000 - 3000 Bit

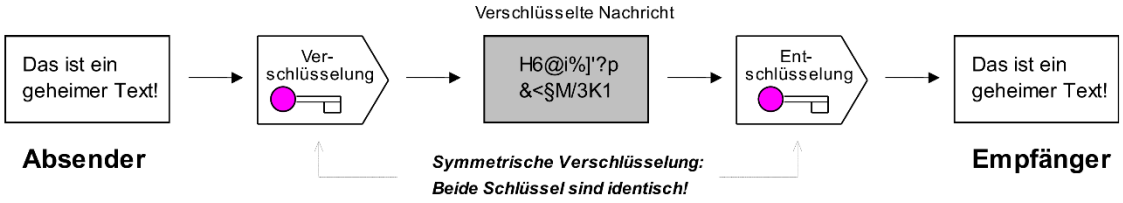
⇒ Probleme

- Schlüsselaustausch bei sym. V.
- hoher Rechenaufwand bei asym. V.

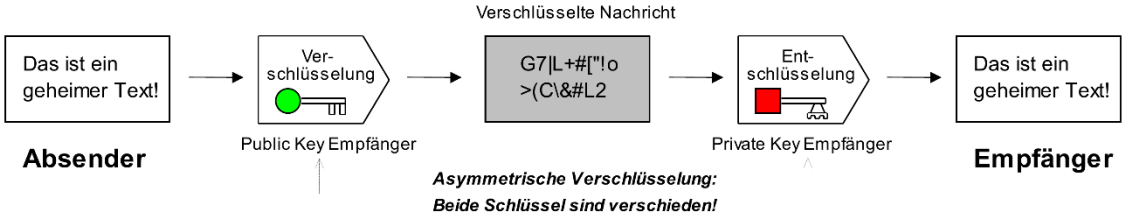
Verschlüsselung wird ***häufig*** eingesetzt!
z.B. bei
- der Übertragung von Webseiten (HTTPS)
- der Übertragung von E-Mails
- Administration entfernter Systeme (SSH)
- WLAN
- VPN
- USB-Datenträger und (Notebooks-)Festplatten

Vergleich Symmetrische/Asymmetrische Verschlüsselung

Symmetrische Verschlüsselung (z.B. AES)

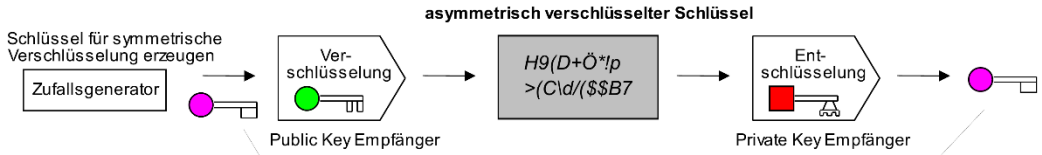


Asymmetrische Verschlüsselung (Public/Private-Key-Verfahren, z.B. RSA)

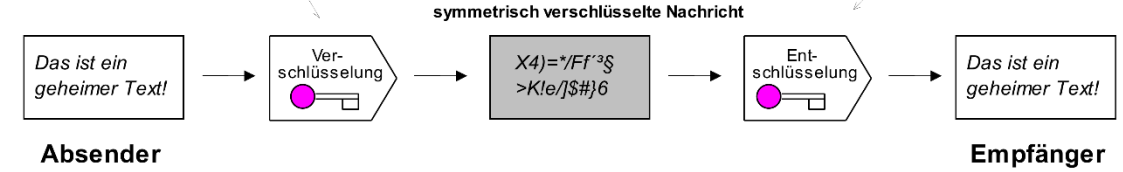


Hybride Verschlüsselungsverfahren

1. Schritt: Schlüssel für symmetische Verschlüsselung erzeugen und diesen mit asymmetrischer Verschlüsselung übertragen



2. Schritt: Nachricht wird mit symmetischer Verschlüsselung übertragen



Einsatz bei: SSH, TLS (IPsec, HTTPS, OpenVPN)

Datenschutz

⇒ ist der gesetzlich geregelte Schutz personenbezogener Daten

⇒ gewährleistet das Recht auf ***informationelle Selbstbestimmung***

⇒ sichert jedem zu, über
- Erhebung, Speicherung,
- Verwendung, Weitergabe

der über ihn gespeicherten Daten **selbst** zu bestimmen

⇒ personenbezogene Daten: sind es dann, wenn die Information einer bestimmten lebenden Person zugeordnet werden kann

⇒ Beispiele: Telefonnummer, E-Mail Adresse, IP-Adresse (*Online-Kennung*), Positionsdaten (*Standortdaten*), KFZ-Kennzeichen, Kontonummer, Unterschrift, Bild einer Person, Zeugnisse, Kaufverhalten, ...

Hinweise dazu: 1, 2

⇒ wichtigste Regelungen: DSGVO, BDSG

Wie funktioniert die DSGVO?

oder: *Mit welchen Prinzipen schützt die DSGVO den Datenschutz?*

⇒ Verbot mit Erlaubnisvorbehalt
Verarbeitung nur, wenn es durch ein Gesetz erlaubt ist oder der Betroffene einwilligt

⇒ Zweckbindung
der vorher festgelegte Verarbeitungszweck darf später nicht verändert werden

⇒ Transparenz
Verarbeitung muss nachvollziehbar sein, Informationspflichten zu Zweck und Umfang

⇒ Datensparsamkeit
Datenmenge muss dem Zweck angemessen und auf das notwendige Maß beschränkt sein

⇒ Sicherheit der Verarbeitung
Vertraulichkeit, Integrität, Verfügbarkeit durch *technische u. organisatorische Maßnahmen* (TOM)

Umsetzung und Kontrolle des Datenschutzes

⇒ durch Datenschutzbeauftragte
- der Bundesbeauftragte für den Datenschutz
- die Landesbeauftragten für den Datenschutz
- betriebliche Datenschutzbeauftragte (DSB)

⇒ Aufgaben des DSB (Artikel 39 DSGVO)
- Unterrichtung und Beratung
- Überwachung der Datenverarbeitung
- Zusammenarbeit mit der Aufsichtsbehörde
- Anlaufstelle für die Aufsichtsbehörde

Verschlüsselung mit 7-Zip

```
:: encrypt.cmd - verschlüsselt alle Dateien im Verzeichnis
@echo off

set "key=qHF*@iDm2W~P!b2X9Df6iqAqy4Er?]"

for %%i in (*) do (
 if /i "%%~nxi" neq "encrypt.cmd" (
   7z.exe a -t7z -mhe -mx0 -sdel -p"%key%" "%%~fi.crypted" "%%~fi" >nul
   if errorlevel 0 echo encrypted: %%~fi
 )
)

pause

:: decrypt.cmd - entschlüsselt alle .crypted Dateien im Verzeichnis
@echo off

set "key=qHF*@iDm2W~P!b2X9Df6iqAqy4Er?]"

for %%i in (*.crypted) do (
 7z.exe e -aoa -p"%key%" "%%~fi" >nul
 if errorlevel 0 (
   echo decrypted: %%~fi
   del /F "%%~fi"
 )
)

pause
```