RBB der Landeshauptstadt Schwerin - Technik -

IT-Sicherheit von Arbeitsplatz-PCc

RBB der Landeshauptstadt Schwerin - Technik -

Informationen stellen für Unternehmen wichtige Werte dar, die geschützt werden müssen. Gefahren drohen beispielsweise durch Offenlegung, Manipulation oder Zerstörung. Da heutzutage die Erstellung, Sammlung, Speicherung, Verarbeitung und Übermittlung von Informationen überwiegend mithilfe von IT erfolgt, ergibt sich für Unternehmen die Notwendigkeit, ihr IT-Umfeld angemessen zu schützen.

Inhalt

IT-Sicherheit

Schutzziele

Gefährdungsfaktoren

Verwundbarkeiten

Angriffsarten

Infektionswege

Maleware

Abwehrmaßnahmen

IT-Sicherheit

Safety

Funktionssicherheit: Ausführen nur vorgesehener und keiner verbotenen Funktionen

und

Security

Informationssicherheit: keine unautorisierte Informationspreisgabe oder –manipulation zulassen

Datensicherheit und Datenschutz

Schutz der Daten selbst und **Schutz personenbezogener Daten**

(Informationstechnisch erfasste, gespeicherte, verarbeitete oder übertragene Informationen bezeichnet man als Daten.)

IT-Sicherheit

In der Datenschutzgrundverordnung (DSGVO) sind folgende Aspekte für die IT-Sicherheit zusammengetragen:

- Funktionssicherheit (safety)
- Informationssicherheit (security)
- Datensicherheit (protection)
- Datenschutz (privacy)
- Verlässlichkeit (dependability)

IT-Geräte sollen **Verlässlichkeit** bieten, also funktionssicher und zuverlässig arbeiten.

Schutzziele

Maßnahmen zum Schutz vor den vielfältigen Bedrohungen zielen auf einen Schutz der IT-Sicherheit ab. Dabei ist es hilfreich konkrete Schutzziele zu untergliedern:

- Vertraulichkeit keine unautorisierte Informationsgewinnung
- Integrität autorisierte und authentifizierte Nutzer können an die Daten
- Verfügbarkeit Personalausweis vorzeigen -> Prüfen auf Echtheit -> ist die Person autorisiert
- Authentizität (Authentisieren, Authentifizieren,Autorisieren) Echtheit der Daten nachvollziehbar z.B. Personalausweiskontrolle
- Verbindlichkeit wenn der Durchführende die Durchführung im Nachhinein nicht abstreiten kann
- Anonymisierung & Pseudonymisierung

Daten weglassen

Daten verfälschen

Gefährdungsfaktoren

Höhere Gewalt

Fahrlässigkeit

Vorsatz

Technisches Versagen

Organisatorische Mängel

Gefährdungsfaktoren (das Risiko)

Das von einer Gefahr ausgehende **Risiko**

bezeichnet die **Wahrscheinlichkeit**, mit der das schädigende Ereignis eintritt, und die **Höhe des möglichen Schadens,** der dadurch hervorgerufen werden kann.

Verwundbarkeiten

Hardwarebasierte Verwundbarkeit

(Fehler im Design Stichwort: Rowhammer)

ROWHAMMER: Speicherzellen werden so manipuliert, das sie benachbarte schädigen können

Softwarebasierte Verwundbarkeiten

Puffer-Überlauf; ungeprüfte Eingaben; kritischer Wettlauf

Infektionswege

Netzwerk

→Drive-by-Download

→E-Mails

→PDF- /Office-Dateien

Benutzer

Externe Speichermedien

-USB-Stick
-Card
-Festplatte
-CD
-…

Computervirus

Ein **Computervirus ist ein sich selbst steuerndes und verbreitendes Computerprogramm**, das in andere auf dem PC installierte Programme eindringt, um sich dort zu reproduzieren. So sind es auch diese Infektions- und Verbreitungsmechanismen, die dem Computervirus seinen aus der medizinischen Klassifizierungsterminologie stammenden Namen *Virus* geben.

Da das zur Kategorie Malware gehörende Computervirus als solches keine eigenen Verbreitungsmechanismen besitzt, ist wie bei seinem biologischen Namensgeber ein sogenanntes Wirtsprogramm erforderlich, das nach erstmaligem Aufrufen seinen vom Entwickler integrierten Schadcode aktiviert, um Programme zum Zwecke der Reproduktion zu infizieren und vorgesehene Schadfunktionen am Betriebssystem, Soft- oder Hardware auszuführen. Harmlose Störungen, aber ebenso größere Datenverluste können die Folge sein.

Merkmale eines Virenbefalls

- Einige Seiten können im Browser nicht mehr angezeigt werden.
- Ihr Computer stürzt in kurzen Zeitabständen ab und startet neu.
- Der Browser öffnet Seiten, die Sie noch nie besucht haben.
- Es erscheinen ungewöhnliche Fehlermeldungen.
- Der Computer wird nach einer Fehlermeldung heruntergefahren.
- Der Computer lässt sich nicht mehr bedienen.

Infektionsarten

Die Infektionsarten unterscheiden sich in der Art, wie ein Virus sich in einem Programm festsetzt

Es gibt drei Infektionsarten:

- über das Booten
- beim Ausführen eines Programmes (*.exe, *.com, usw.)
- über infizierte Dokumente

Beispielsweise hängen viele Viren ihren eigenen Programmcode an das Ende einer ausführbaren Datei und setzen am Anfang einen Zeiger auf diesen Code. Wird das Programm gestartet, springt es vor der Ausführung seiner eigentlichen Aufgaben zuerst auf das Virusprogramm. Ist dieses ausgeführt, springt es wieder an die Stelle zurück, an der der Ablauf ursprünglich unterbrochen wurde. Sie merken dann nicht einmal, dass sich das Aufrufen des Programms minimal verzögert hat. Rufen Sie das Programm jetzt auf, startet zuerst der Virus. Er sucht von diesem Moment an nach nicht infizierten, ausführbaren Dateien, um diese auch noch zu befallen.

Aufbau von Viren

- Erkennungsteil:
  Hier wird geprüft, ob ein Programm bereits infiziert wurde. Ist das der Fall, kann auf eine erneute Infektion verzichtet und stattdessen ein anderes Programm infiziert werden. Auf diese Weise wird die Verbreitung des Virus beschleunigt.

- Bedingungsteil:
  Sowohl die Verbreitung eines Virus als auch dessen zu verursachende Schäden können an bestimmte Bedingungen geknüpft sein. Der „Michelangelo"-Virus überschreibt beispielsweise nur am 6. März jeden Jahres die Festplatte mit zufällig ausgewählten Zeichen. Der Bedingungsteil kann fehlen.

- Schadensteil:
  Im Schadensteil sind die eigentlichen zu verursachenden Schäden wie z. B. das Löschen von Dateien programmiert. Der Schadensteil ist nicht zwingend vorhanden, jedoch stellt die alleinige Inanspruchnahme von Speicherkapazität durch einen Virus auch bereits einen Schaden dar.

- Tarnungsteil:
  Das Tarnen eines Virus soll dessen Entdeckung im infizierten System erschweren. Auch dieses Element ist kein notwendiger Virenbestandteil.

- Reproduktionsteil:
  In diesem Programmteil wird die Fortpflanzung des Virus durchgeführt.

Angriffsarten

Passive Angriffe

(Sniffer- Angriffe)

Aktive Angriffe

(Spoofing-Angriffe oder Denial-of-Service-Angriffe (DoS-Angriffe)

Virenarten

- Bootvirus

Bootviren schreiben sich in den Bootsektor von Festplatten, Disketten oder Speicherkarten beziehungsweise -sticks. Sie werden aktiv, sobald der Computer von solch einem infizierten Datenträger gestartet wird. Daher sollte man nie eine Diskette beim Ausschalten des PCs im Laufwerk vergessen.

- Makroviren

Makroviren brauchen als Wirt Dateien, die Makros enthalten können, beispielsweise Word- und Excel-Dateien. Die Schadmakros werden beim Öffnen der Datei automatisch mitgestartet und spulen dann ihre Befehle ab.

- Skriptviren

Skriptviren befallen Skripte, die zum Beispiel in vielen Internetseiten eingebaut sind. Sie sind oft in der Programmiersprache „Javascript“ geschrieben. Denn diese Sprache verstehen die gängigen Internet- Browser, zum Beispiel der Internet Explorer. Die führen dann das schädliche Skript aus, und schon ist der PC infiziert.

Virenarten

- Programmviren

Programmviren brauchen als Wirt ein Programm (Datei-Endung „.exe“, „.com“ oder „.dll“). Sie werden aktiviert, wenn eine befallene Datei ausgeführt wird.

- Hybridviren (Multipartite Viren)

Hybridviren sind Kombinationen von mehreren Virenarten. Damit machen sie sich verschiedene Ausbreitungsmethoden gleichzeitig nutzbar und sind somit schwerer aus dem System zu entfernen. Sie vereinen oft Virenmethodik mit Hackerangriffen und besitzen dadurch ein noch höheres Schadenspotenzial.

- Stealth-Viren (Tarnkappenviren)

Stealth-Viren sind Viren mit speziellen Mechanismen, sich vor Virensuchprogrammen zu verstecken. Sie können z. B. eine infizierte Datei vor der Überprüfung restaurieren und somit die Verseuchung unkenntlich machen.

Andere Malware

• Würmer

Würmer sind keine Viren im eigentlichen Sinne, da sie keine Wirtsprogramme benötigen, sondern ausschließlich sich selbst kopieren.

• Trojanische Pferde

Trojanische Pferde (Trojaner) sind auch keine Viren im eigentlichen Sinne (da sie sich i. d. R. nicht selbst reproduzieren), sondern Programme mit Virenfunktionalität, die sich hinter dem Namen von bekannter (harmloser) Software verstecken. Der Begriff Trojaner wird oftmals synonym für Spionage-Software verwendet. Besondere Kennzeichen sind, dass sie oftmals lange Zeit unentdeckt bleiben und von „innen nach außen“ wirken.

• Denial-Of-Service (E-Mail-Bombing)

Beim E-Mail-Bombing überhäuft ein Angreifer ein Zielsystem mit Mails, so dass im Extremfall die normale Nutzung von Mail nicht mehr möglich ist.

Andere Malware

• Phishing

Unter **Phishing** versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen und den entsprechenden Personen zu schaden. Es handelt sich dabei um eine Form des Social Engineering, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird.

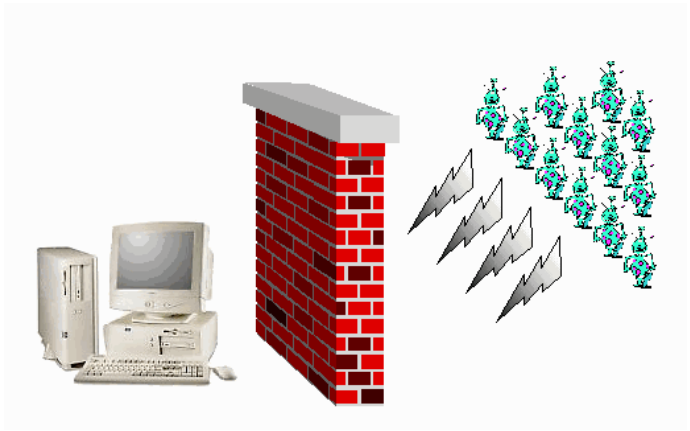
• Rootkit

Ein **Rootkit** ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Softwaresystem auf dem kompromittierten System installiert wird, um zukünftige Anmeldevorgänge des Eindringlings zu verbergen und Prozesse und Dateien zu verstecken.

Malware

- Spyware
- Adware
- Bot, Bot-Netz
- Ransomware Verschlüsselung
- Scareware Verunsichern

Abwehrmaßnahmen



Abwehrmaßnahmen

Verschlüsselung

Digitale Signatur

Hash Funktionen

Beschränkung der Nutzerrechte

Monitoring

Nachwirkungen von Datenschutzverletzungen Nachvollziehen

Passwort-Manager

Passwortlose Anmeldung mit FIDO2

Zweifaktor-Authentifikation