Arbeitsdossier - Begriffe in der IT-Sicherheit

182 - Systemsicherheit implementieren

Grundlagen

Die IT-Security kennt diverse spezifische Begrifflichkeiten. Die folgenden Aufgaben sollten Ihnen Klarheit verschaffen, wann welcher Begriff wo zur Anwendung kommt.

Die absolute Grundlage in der IT-Security ist CIA!

Recherchieren Sie kurz die Bedeutung der drei Buchstaben und beantworten Sie die nachfolgenden Fragen:

Für was steht das "**C**" Englisch: Confidentiality . Deutsch: Vertraulichkeit
Für was steht das "**I**" Englisch: Integrity . Deutsch: Integrität
Für was steht das "**A**" Englisch: Availability . Deutsch: Verfügbarkeit

Was wird bei HTTPS realisiert? ☒ C ○ I ○ A

Was wird mit einer USV realisiert? ○ C ○ I ☒ A

Was realisiert eine E-Mail-Verschlüsselung? ☒ C ○ I ○ A

Was ist Sicherheit und welche zwei Formen von Sicherheit gibt es?

Wie lautet die Definition des Begriffs "Sicherheit"?

Zustand des Sicherseins, Geschütztseins vor Gefahr oder Schaden; höchstmögliches Freisein von Gefährdungen

---

In welchem Kontext kommt der Begriff **Security** zum Einsatz?

Bei der Physischen sicherheit, wie Gebäude oder Personen sicherheit werden die Sichernden Personen meist als Security bezeichnet

In der IT wird die CyberSecurity auch als Security bezeichnet

---

In welchem Kontext kommt der Begriff Safety zum Einsatz?

.....

.....

.....

Übung 1

Bilden Sie Zweier-Teams und bearbeiten Sie folgende Szenarien:

Szenario 1

Eigenschaften eines Systems der IT, dass nur Berechtigten (Kommunikationspartnern) bestimmte Daten, Dienstleistungen und Betriebsmittel (Objekte) verfügbar gemacht werden und Unberechtigten der Zugriff auf Objekte verwehrt wird. Schutz vor unberechtigtem Zugriff auf Daten und Ressourcen.

Nennen Sie die betroffene CIA-Disziplin: Vertraulichkeit

Was ist die eigentliche Bedrohung: Unberechtig oder Dritte verschaffen sich Zugriff

Wie könnte man sich schützen: Detailiertes Berechtigungs und Zugriffkonzept

Szenario 2

Eigenschaft von Daten, Dienstleistungen und Betriebsmitteln, immer dann verfügbar sein, wenn ein autorisierter Benutzer sie bearbeiten bzw. in Anspruch nehmen will; "Verfügbar" heisst dabei "Zugriff ist in akzeptabler Zeit möglich". Geräte und Programme sollen zur Nutzung uneingeschränkt zur Verfügung stehen; Schutz vor unbefugter Beeinträchtigung der Funktionalität.

Nennen Sie die betroffene CIA-Disziplin: Availability

Was ist die eigentliche Bedrohung: Beeinträchtigung der Funktionalität durch Einflüsse von Aussen und Innen

Wie könnte man sich schützen: Redundanz

Szenario 3

Informationen und Prozesse zu ihrer Verarbeitung sind gemäss den definierten Vorgaben abrufbar respektive durchführbar; und zwar am richtigen Ort und in der vorgegebenen Form.

Nennen Sie die betroffene CIA-Disziplin: Integrität

Was ist die eigentliche Bedrohung: Fasche verarbeitung der Daten durch Schnittstellen oder Mitarbeiter

Wie könnte man sich schützen: Klare Prozesse und vollständige Daten

Übung 2

Wechseln Sie bitte Ihren Team-Partner bzw. Ihre Team-Partnerin.

Die IT-Sicherheit stützt sich auf die drei Grundsäulen C I A. Nebst diesen drei Hauptargumenten gibt es jedoch noch diverse andere wichtige Ankerpunkte, welche C I A zu unterstützen vermag. Erinnern Sie sich bitte an die vergangenen Lehrjahre (bzw. Module) … Sie sollten nämlich sämtliche zusätzlichen Punkte kennen (als Beispiel ist der letzte Punkte bereits ausgefüllt):

Punkto Datenhaltung 1 (Modul 143): .....

Punkto Datenhaltung 2 (Modul 143): .....

Punkto Benutzer-Überprüfung (Modul 159): .....

Punkto Berechtigungen (Modul 157): .....

Punkto Verbindlichkeit (Modul 145): *Non-Repudiancy (auditability, logging, monitoring)*

Übung 3

Bleiben Sie in Ihrem Team und überlegen bzw. nennen Sie zwei Angriffsszenarien auf eine ICT-Infrastruktur und beschreiben Sie eine technisch korrekte Gegenmassnahme. Fokussieren Sie sich dabei nur auf die behandelte Thematik. Weitere Szenarien folgen im Verlaufe des Unterrichts:

Angriff 1: .....

.....

.....

Schutz 1: .....

.....

.....

Angriff 2: .....

.....

.....

Schutz 2: .....

.....

.....

Abschluss Grundlagen

Zusammenfassend für das erste Kapitel, hier die Definition des BSI betreffend IT-Sicherheit:

„IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Massnahmen auf ein tragbares Mass reduziert sind. IT-Sicherheit ist also der Zustand, in dem ***Vertraulichkeit****,* ***Integrität*** *und* ***Verfügbarkeit*** *von Informationen und Informationstechnik durch angemessene Massnahmen geschützt sind.“*

Persönliche Notizen zu diesem Kapitel

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Bedrohungen und deren Charaktere

Was wäre der Wirtschaftszweig „**Security/Safety**“ ohne äussere Einflüsse? Sicherlich könnte man mit guten Marketing-Kampagnen einen bescheidenen Absatz/Umsatz sicherstellen… ob das Geschäft jedoch jemals zu florieren beginnen würde, gilt es zu bezweifeln.

Bevor wir mit diesem Thema starten, sollten Sie sich bewusst sein, dass nicht jedes Ereignis aufgrund böser Absichten zustande kommt. Wir unterscheiden primär drei Vorkommnisse:

- ***Höhere Gewalt***
- ***Unwissenheit/Fahrlässigkeit***
- ***Mutwilligkeit***

Wenn Sie sich nun die potenziellen Gefahren betrachten, welche Punkte können wann erfüllt sein?

Eine nicht autorisierte Person erlangt Zugriff, auf für Sie nicht bestimmte, Daten.

○ Höhere Gewalt ○ Fahrlässigkeit ○ Mutwilligkeit

Daten, Prozesse und/oder Dienstleistungen sind nicht verfügbar.

○ Höhere Gewalt ○ Fahrlässigkeit ○ Mutwilligkeit

Daten, Prozesse und/oder Dienstleistungen werden geändert.

○ Höhere Gewalt ○ Fahrlässigkeit ○ Mutwilligkeit

Daten in einer automatisierten/prozessgesteuerten Passwortverwaltung werden manuell hinzugefügt.

○ Höhere Gewalt ○ Fahrlässigkeit ○ Mutwilligkeit

Verfügbarkeit der Serverinfrastruktur ist aufgrund Löschwasser (Kurzschluss) nicht gegeben.

○ Höhere Gewalt ○ Fahrlässigkeit ○ Mutwilligkeit

Ein Servertechniker arbeitet ohne elektrostatischem Armband und verursacht Kurzschluss auf Mainboard.

○ Höhere Gewalt ○ Fahrlässigkeit ○ Mutwilligkeit

Script-Kiddy führt während Schnupper-Lehre ein Skript aus, welches die Server abstürzen lässt.

○ Höhere Gewalt ○ Fahrlässigkeit ○ Mutwilligkeit

Zusammenfassend kann gesagt werden, dass sich folgende potenziellen Angriffe innerhalb einer ICT-Infrastruktur wie folgt identifizieren lassen (höhere Gewalt wird bewusst geklammert):

Abfangen, Mithören, Spionage
Eine nicht autorisierte Person erlangt Zugriff auf Daten bzw. Systeme

→ zum Beispiel: *Illegale Kopie von Daten*

Unterbrechung
Daten, Prozesse oder Dienstleistungen sind nicht verfügbar, werden zerstört oder unbrauchbar.

→ zum Beispiel: *Daten sind korrupt oder verloren, Denial of Service*

Modifikation, Veränderung, Sabotage
Daten, Prozesse oder Dienstleistungen werden geändert bzw. manipuliert.

→ zum Beispiel: *Daten bei der Übertragung ändern*

Aus solchen Vorkommnissen entstehen natürlich aus Schäden. Im Bereich des Risikomanagements spricht man hier von drei Kategorien:

Direkte Schäden
An Maschinen, Datenträgern, Daten, Systemen, Gebäuden, etc.

Indirekte Schäden
Ersatzbeschaffungen, Rekonstruktion von manipulierten Daten, Personalaufwand, etc.

Folgekosten
Entgangene Umsätze/Gewinne, Schadensersatzansprüche von Dritten, Imageschaden, etc.

Deklarieren Sie für das folgende Szenario, welche Bedrohung einwirkte, und welcher Schaden effektiv entstanden ist. Nehmen Sie bitte schriftlich Stellung:

14.03.2016 (Quelle: www.watson.ch) – ***Grossangriff auf SBB, Interdiscount, Digitec, Galaxus und Microspot****. … es deutet einiges darauf hin, dass es sich um einen grossflächigen Angriff auf den Schweizer E-Commerce handelt …*

Bedrohung/Angriff: .....

.....

.....

.....

Schaden/Schäden: .....

.....

.....

.....

Aufgabe 1

Umschreiben Sie bitte folgende Begrifflichkeiten. Nutzen Sie hierfür sämtliche zugängliche Medien, um eine möglichst exakte Begriffsdeklaration zu erhalten.

White Hat: .....

.....

.....

.....

Grey Hat: .....

.....

.....

.....

Black Hat: .....

.....

.....

.....

Script Kiddy: .....

.....

.....

.....

Malware: .....

.....

.....

.....

Virus: .....

.....

.....

.....

Wurm: .....

.....

.....

.....

Aufgabe 2

Bilden Sie nun wieder 2er-Teams. Diskutieren Sie über die Motive von Cyber-Kriminellen und versuchen Sie deren Beweggründe nach folgenden Punkten zu charakterisieren:

Politische Motive

Wirtschaftliche Motive

Persönliche Motive