Abgabe Gruppe 1, Veriefung 1

Aufgabe a) Safety und Security

Stellen Sie die Safety der Security gegenüber. Betrachten Sie dabei folgende Aspekte:

- Einsatzbereiche
- Normen
- Bedrohung
- Schwachstelle
- Schutzobjekt
- Schutzziele, z.B. CIA

Antwort

Unter dem Begriff Safety betrachtet man Sicherheit unter dem Aspekt Unfallvermeidung bzw. Betriebssicherheit. Im Falle von Security betrachtet man das Verhindern, meist strafbarer, Handlungen. Safety Konzepte kommen vor allem dort zum einsatz wo es um den Schutz von Leib und Leben geht, Securitykonzepte im Bereich wo es um den Schutz von Daten und ITK-Systemen geht. Einschlägige Normen zum Themen Safety sind z.B:

- ISO/IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
- EN ISO 12100:2010: Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung
- Richtlinie 2006/42/EG: "Maschinen Richtlinie" (wird zur Zeit überarbeitet)

Diese Richtlinien beschäftigen sich alle mit der sicheren Auslegung und Betrieb von Maschinen, meist im industriellen Umfeld. Allen gemeinsam ist das sie IT Security nicht, oder nur sehr eingeschränkt behandeln.

Im Bereich (IT) Security findet man unter anderem folgende Standards:

- ISO/IEC 2700x Familie: Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme ff. [^1]
- SOC2: Service Organization Control 2 [^2]
- IT-Grundschutz-Kataloge des BSI [^3]

Welche sich vornehmlich auf IT Systeme beziehen, aber eine Bezug zu technischen System missen lassen.

Eine Bedrohung stellt eine abstrakte Gefahr dar, welche potenziell denkbar ist. Eine Schwachstelle eine konkret ausnutzbare Lücke.

Schutzobjekte können einzelne Systeme oder Programme aber auch Räumlichkeiten darstellen [^4]. Bei Safety würde man hier sprechen wenn es um Aspekte wie Arbeitsschutz geht. Bei Security hingegen wenn es um Dinge wie Zugangskontrolle oder Rechte geht. Schutzziele im Sinne von Security können unteranderem sein:

- C: Vertraulichkeit (Confidentiality): Systeme sollen sollen u.A. sicher gegenüber abhören sein und pseudonym nutzbar sein
- I: Intigrität (Integrity): Systeme sollen korrekt arbeiten
- A: Verfügbakeit (Availability): Systeme sollen erreichbar sein

Bei Safety wird Sicherheit unter dem Schutz von Leib und Leben betrachtet, z.B das vermeiden von UNfällen welche zu Gesundheitsschäden führen können.

Aufgabe c) Risiko - Wie kann ein Sicherheitsrisiko berechnet werden?

Ein Sicherheitsrisiko lässt sich wie folgt berechnen: Risiko = Auswirkung x Eintrittswahrscheinlichkeit

Hierbei können folgende Kategorien für Eintrittswahrscheinlichkeiten angenommen werden[^5]:

- sehr wahrscheinlich: einmal pro Woche oder öfter,
- wahrscheinlich: einmal pro Monat,
- möglich: einmal pro Jahr,
- unwahrscheinlich: alle 10 Jahre oder seltener. Schadenskategorien[^6]:
- niedrig: geringe, kaum spürbare Auswirkung
- normal: spürbare Auswirkungen auf den Betrieb
- hoch: erhebliche Auswirkungen Auf den Betrieb
- sehr hoch: Ausfall/Beeinträchtigung welche sich existentiell bedrohlich auswirkt.

Daraus ergibt sich die folgende Matrix für Risiken und ihre Bewertung:

	Niedrig	**Mittel**	**Hoch**	**Sehr hoch**
Sehr wahrscheinlich	gering	mittel	hoch	sehr hoch
wahrscheinlich	gering	mittel	hoch	hoch
Möglich	gering	gering	mittel	mittel
Unwahrscheinlich	gering	gering	gering	gering

Aufgabe d) Security-Vorgehensweise

Warum möchte man in der Security-Analyse eine Bedrohung gar nicht vermindern? Wann kommen Safety-Maßnahmen zum Einsatz? Warum will man die Bedrohung hier vermindern?

Im Rahmen von Security-Analysen wird nur der Angriffspfad auf das System analysiert. Safty Maßnahmen kommen zum einsatz wenn es sich um Fehler im System handelt, welche behoben werden Können. Hierbei können Bedrohungen durch beheben der Fehler behoben werden, da, im gegensatz zur Security, kein aktiver Gegenspieler vorhanden ist.

Aufgabe e) Maßnahmen

Warum werden die entdeckten Schwachstellen nicht sofort behoben?

Schwachstellen werden zuerst priorisiert. Faktoren die dafür eine Rolle spielen könnten:

- Wird die Schwachstelle bereits aktiv ausgenutzt?
- Handelt es sich um eine kritische Lücke deren potenziellen Ausnutzung kritischen Schaden anrichtet?
- Sind arbeiten in dem Bereich geplant?
- Gibt es regulatorische Pflichten?

Und viele mehr.

Nach erfolgter Priorisierung erfolgt dann eine Abarbeitung.

Aufgabe f) Störungsmanagement

Stellen Sie Störungen, Notfälle, Krisen und Katastrophen gegenüber. Wie werden sie in großen Organisationen gehandhabt? Wie ist Resilienz definiert? Worum geht es beim Wiederanlauf? Wo erfolgt die Beobachtung der IT? Wer kümmert sich um Notfälle? Wo werden die Lagebilder aufbereitet? Wer fällt in Krisen Entscheidungen?

Störungen, Notfälle, Krisen und Katastrophen sind Ereignisse, die sich auf unterschiedliche Weise auf eine Organisation auswirken können. Störungen sind in der Regel geringfügige Probleme, die schnell behoben werden können und keine weitreichenden Auswirkungen auf die Organisation haben. Notfälle hingegen erfordern sofortiges Handeln, um Schäden zu begrenzen. Krisen sind langanhaltende und schwerwiegende Ereignisse, die die Organisation stark belasten können. Katastrophen sind außergewöhnliche Ereignisse wie Naturkatastrophen, die zu massiven Schäden führen können.

In großen Organisationen werden Störungen, Notfälle, Krisen und Katastrophen in der Regel durch einen Krisenstab oder eine Krisenmanagement-Abteilung gehandhabt. Im Falle von IT (Security) von einem CERT (Computer Emergency Response Team). Diese Abteilung ist verantwortlich für die Überwachung der Situation, die Entscheidungsfindung und die Koordination der Maßnahmen zur Bewältigung der Krise. Man spricht in diesem Rahmen auch von BCM (Business Continuity Management).

Resilienz bezieht sich auf die Fähigkeit einer Organisation, Krisen und Veränderungen zu bewältigen und sich schnell zu erholen. Eine resiliente Organisation kann schnell auf unvorhergesehene Ereignisse reagieren und sich schnell anpassen.

Beim Wiederanlauf geht es darum, die Geschäftstätigkeit nach einem Notfall oder einer Krise so schnell wie möglich wieder aufzunehmen. Dazu müssen die IT-Systeme wiederhergestellt werden und andere geschäftskritische Systeme müssen wieder in Betrieb genommen werden.

Die Beobachtung der IT erfolgt in der Regel durch spezialisierte IT-Abteilungen, die auf die Überwachung von Systemen und die Erkennung von Störungen und Sicherheitsproblemen spezialisiert sind.

Notfälle werden von verschiedenen Abteilungen in der Organisation gehandhabt, je nach Art des Notfalls. In der Regel gibt es jedoch eine Krisenmanagement-Abteilung, die für die Koordination der Maßnahmen verantwortlich ist.

Lagebilder werden in der Regel von der Krisenmanagement-Abteilung oder dem Krisenstab aufbereitet. Hier werden alle Informationen über die Krise gesammelt und analysiert, um eine fundierte Entscheidungsfindung zu ermöglichen.

In Krisen werden Entscheidungen in der Regel vom Krisenstab oder der Krisenmanagement-Abteilung getroffen. Hier werden alle verfügbaren Informationen gesammelt und analysiert, um fundierte Entscheidungen zu treffen. Je nach Art der Krise können auch Führungskräfte aus anderen Abteilungen hinzugezogen werden, um bei der Entscheidungsfindung zu helfen.

Quellen

---

^1: Iso 270xx Fammilie ^2: SOC2 ^3: IT Grundschutz Kataloge ^4: Schutzobjekte ^5: Schadenskategorien ^6: BS1 Standard 200-1