MUSTERLÖSUNG, H.P. KÖNIGS, SPRINGER VIEWEG „IT-RISIKOMANAGEMENT MIT SYSTEM“, 5. AUFLAGE

KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 17

Lösung zu Frage 1

Cyber-Risiko kann wie folgt definiert werden:

> *Ein Cyber-Risiko ist ein Risiko, das durch eine Cyber-Bedrohung verursacht wird. Dabei nutzen die Cyber-Bedrohungen den Cyberspace aus.*

Diese Definition benützt den Begriff Cyberspace, der durch den US-amerikanischen Standard NIST Special Publication 800-30 Revision 1, sinngemäss wie folgt definiert ist:

> *Cyberspace ist ein globaler Bereich in der Umgebung von Informationen; dieser besteht aus einem ineinandergreifenden Netzwerk von Informationssystem-Infrastrukturen, einschliesslich dem Internet, den Telekommunikationsnetzwerken, den Computer-Systemen und den eingebetteten Prozessoren und Kontrollern.*

Lösung zu Frage 2

Im US-amerikanischen Standard NIST Special Publication 800-30 Revision 1 werden haben die Charakteristiken die folgenden Attribute:

- Die **Bedrohungsquellen** bei den absichtlichen Risiken werden mit den folgenden Attributen charakterisiert:
  - Fähigkeit
  - Absicht und
  - Angriffsziele
- Die **Bedrohungsereignisse** bei den absichtlichen Risiken werden mit den folgenden Attributen charakterisiert:
  - Taktiken
  - Techniken und
  - Verfahren

Lösung zu Frage 3

Bedrohungsquellen für absichtliche Bedrohungen (adversarial threats) können sein:

- Staatliche Institution
- Verbrecherbande
- Wettbewerber
- Privilegierter Insider-Betrüger
- Terrorist mit politischem Hintergrund

Bedrohungsquellen für unabsichtliche Bedrohungen (non-adversarial threats) können sein:

- Hochwasser
- Feuer

- Verkehrsunfall
- Fehlfunktionen technischer Geräte
- Benutzerfehler

Lösung zu Frage 4

Beispiel **Bedrohungsereignis:** Ausnützen von unlängst aufgedeckten Schwachstellen resp. Exploits.

Beschreibung: Ein Angreifer (Bedrohungsquelle) nützt durch das Einschleusen eines entsprechenden Programmcode eine unlängst bekannt gewordenen Schwachstelle im Betriebssystem einer betrieblichen Anwendungssoftware aus.

Lösung zu Frage 5

Im folgenden Ablauf werden die Aktivitäten der Identifikation und Analyse eines Risikos beginnend mit der Benennung und Nummerierung des Risikos beschrieben. Der Ablauf endet mit der Bestimmung des Risikos aus der Eintrittswahrscheinlichkeit und dem Schadensausmass.

Schritt	Aktivität
1.	Risiko benennen und nummerieren.
2.	Risikoobjekt (asset) identifizieren: System, Prozess, Organisations-Ebene etc.
3.	Bedrohungsereignis (threat event) identifizieren.
4.	Bedrohungsquellen (threat sources) identifizieren, welche das Bedrohungsereignis auslösen können.
5.	Charakterisierung der Bedrohungsquellen für: • **Absichtlich** herbeigeführte Risiken (z. B. durch Hacker oder Datendiebe): Charakterisierung durch Einstufung deren Fähigkeiten, Absichten und Angriffsziele; • **Unabsichtlich** herbeigeführte Risiken (z. B. Unfall oder Unwetter): Charakterisierung durch Einstufung deren potentiellen Wirkungsbereiche.
6.	Relevanz des Bedrohungsereignisses einstufen.
7.	Schwachstellen (vulnerabilities) identifizieren, welche von den Bedrohungsquellen durch das Auslösen entsprechender Bedrohungsereignisse ausgenützt werden, um das Eintreten von Schäden zu ermöglichen.
8.	Ernsthaftigkeit der Schwachstellen einstufen.
9.	Wahrscheinlichkeit **p1** einstufen, dass ein Bedrohungsereignis durch eine oder mehrere der Bedrohungsquellen, unter Beachtung deren Charakteristiken (s. Schritt 5), ausgelöst wird.
10.	Wahrscheinlichkeit **p2** einstufen, dass ein durch die Bedrohungsquellen ausgelöstes Bedrohungsereignis, unter Berücksichtigung der Charakteristiken der Bedrohungsquellen sowie der Schwachstellen, zu einem Schaden (Impact) führt.
11.	Wahrscheinlichkeit (Eintrittswahrscheinlichkeit) **P = f(p1,p2)** ermitteln, dass ein ausgelöstes Bedrohungsereignis auch zu einem Schaden führt (Kombination von p1 und p2).
12.	Höhe des Schadens (Impact) **S** am Risikoobjekt aufgrund des Bedrohungsereignisses einstufen.
13.	Höhe des Risikos **R = f(P,S)** aufgrund der Kombination der Eintrittswahrscheinlichkeit P und der Höhe des Schadens S bestimmen.

Der oben gezeigte Ablauf erfolgt induktiv, d.h. von der Kenntnis und Einstufung der Bedrohungsquellen her, über die möglichen Bedrohungsereignisse und die vorhandenen Schwachstellen bis hin zur Bestimmung des Risikos in seiner Höhe. Oft fehlen in einer solchen Assessment-Kette Informationen, z.B. über die möglichen Bedrohungsquellen; deshalb ist manchmal auch eine deduktive Vorgehensweise sinnvoll, z.B. von den möglichen Schäden, die sich bei der vorhandenen Konstellation der Assets und den allenfalls vorhandenen Schwachstellen ergeben, zurück zu den möglichen Bedrohungsereignissen und den noch weiter zurück liegenden möglichen Quellen, die überhaupt in der Lage sein könnten, entsprechende Risikoereignisse auszulösen. Sicherlich werden mögliche Risikoereignisse und die entsprechenden Massnahmen durch allfälliges Hin- und Herwechseln zwischen induktiven und deduktiven Vorgehensweisen am besten ermittelt und analysiert werden können.

Lösung zu Frage 6

Allgemeine Beschreibung von **Advanced Persistent Threats (APT):**

Unter APT wird eine hoch entwickelte Bedrohung verstanden, bei der die Bedrohungsquelle sowohl über eine hohe Expertise als auch über signifikante Ressourcen verfügt, um mittels mehreren geeigneten Taktiken, Techniken und Verfahren die angestrebten Angriffsziele zu erfüllen. Solche Angriffsziele lassen sich typischerweise durch Vordringen in die Informationsinfrastruktur (Server, Datenbanken etc.) einer Organisation zum Zwecke des Ausspähens sensibler Daten oder zu anderweitigen Schädigungen des Opfers erfüllen. Dabei setzt der Angreifer seine Angriffsziele unbemerkt und über eine grössere Zeitspanne um und widersetzt sich dabei in geeigneter Weise den Verteidigungsbemühungen der angegriffenen Organisation. Der fortgesetzte Angriff wird meist durch die Installation eines Backdoors beim erstmaligen Eindringen und mit nachfolgenden lateralen Verschiebungen im Netzwerk mit weiteren Backdoor-Installationen erreicht. Die dabei verwendeten Angriffscodes werden meist fortlaufend auf die aktuelle Situation angepasst, um Angriffsziele und Opportunitäten umzusetzen und dabei nicht entdeckt zu werden. Für Angriffskampagnen entwickeln die Angreifer oft spezielle noch unbekannte Malware (Exploits), um bisher unbekannte Schwachstellen auszunutzen. Solche Malware wird bei ihrem Auftreten als „Zero-day exploit“ bezeichnet.

Oft eingeschlagene Vorgehensweise der **Advanced Persistent Threats**:

1. Ausspähung und Erkundung des Zielobjekts;
2. Planung;
3. Ausnutzung von Schwachstellen, Infiltration und Vordringen in das Zielobjekt;
4. Übernahme der Steuerung des Zielobjekts;
5. Erhöhung der Privilegien und Zugriffsrechte und sukzessive Übernahme der Kontrolle über das Zielobjekt;
6. Seitenbewegungen und Einbezug zufälliger Ziele;
7. Umsetzung des gesetzten Ziels und Einrichtung einer beständigen Kontrolle über Funktionen des Zielobjekts;
8. Verwischen der Spuren.

Lösung zu Frage 7

Die Cyber-Risiken, insbesondere die absichtlichen, bestehen oft aus mehreren Einzelrisiken, die oft mit spezifischen einzelnen Bedrohungen oder einzelnen Schwachstellen gegenüber gestellten Massnahmen nicht behoben werden können. Dies rührt u. a. auch daher, dass über die möglichen Bedrohungsquellen und ihren Absichten, Motivationen und Fähigkeiten meist wenig bekannt ist. Auch weisen die auf bestimmte Organisationen oder Risikoobjekte abzielenden Cyber-Risiken bezüglich der beabsichtigten Bedrohungsereignisse eine hohe Variabilität auf. Die einzusetzende Palette von Massnahmen muss demzufolge entsprechend breit sein und dynamisch wirken, um der Vielfalt möglicher Angriffe und deren Dynamik Rechnung tragen zu können. Somit wird sich bei Organisationen, die sich gegen Cyber-Risiken widerstandsfähig machen wollen, eine Art Grundschutz (Baseline Security) gegen Cyber-Risiken aufdrängen, wobei dieser Grundschutz der Dynamik und der Innovation möglicher Cyber-Angriffe gewachsen sein muss. Selbstverständlich bedarf es zusätzlich zum Cyber-Sicherheits- Grundschutz noch spezifische Massnahmen, welche die Eigenheiten der Organisation bezüglich ihrer speziellen Exposition (z. B. hinsichtlich Datenlecks oder kritischer Infrastrukturen) berücksichtigen muss. Doch sollte ein Grundschutz mit gegen Cyber-Risiken prädestinierten Massnahmen, wie Malware-Scanner, Sichere Authentisierung, Zugriffskontrolle, als Minimum zur Erlangung von Cyber-Sicherheit angesehen werden.

Lösung zu Frage 8

Sämtliche Massnahmen gegen mögliche Cyber-Risiken, denen ein Unternehmen ausgesetzt werden könnte, sind in einem Unternehmen nicht umsetzbar. Dies gilt sowohl hinsichtlich der Massnahmen-Kosten, des Betreuungsaufwands als auch für die Anpassung der Prozesse an die aktuelle Risikosituation. Aufgrund der möglichen Schäden, z.B. bei der Kompromittierung von Daten des Unternehmens oder bei der Störung von Geschäfts- und Betriebsabläufen, ergeben sich vielmehr unterschiedliche Wichtigkeiten, Prioritäten und Spezifikationen für die Massnahmen. Somit sind für die dem Unternehmen eigenen Cyber-Risiken und sonstigen Anforderungen entsprechend angemessene und angepasste Massnahmen einzusetzen. Solche risikobasierten Massnahmen können auch als sinnvolle Komplementierung eines Grundschutzes gegenüber Cyber-Risiken angesehen werden.

Lösung zu Frage 9

Ein ISMS behandelt die aktuelle Sicherheitslage im Unternehmen resp. im definierten Anwendungsbereich des ISMS. Somit wird ein gut geführtes ISMS auch den Cyber-Risiken bestmöglich gerecht werden können. Die aufgrund spezifischer Risiken zu ergreifenden Massnahmen in einem ISMS dienen somit nicht nur der Vorbeugung gegen das Eintreten von Risiken, sondern behandeln auch die Massnahmen und Vorgehensweisen, falls ein Cyber-Risiko-Ereignis tatsächlich eingetreten ist.

Lösung zu Frage 10

Das „Incident Response Team“ (IRT) besteht meist aus einer Gruppe von Fachpersonen, welche die Vorbereitungen für die Behandlung möglicher Ereignisfälle trifft und beim tatsächlichen Eintritt eines Ereignisses (z.B. unerwünschte Systemunterbrechung oder

Geschäftsprozess-Unterbrechung) sich der Lösung des eingetretenen Problems hinsichtlich einer möglichst geringfügigen Schadensauswirkung annimmt. Die Mitgliedschaft in einem „Incident Response Team“ ist im Unternehmen oft als Nebenaufgabe definiert, doch bedürfen die Mitglieder, aufgrund der hohen Anforderungen, entsprechender Schulungen und Übungen. Die anfallenden Aufgaben erfordern meist auch ein Mass an interdisziplinären Kenntnissen im Unternehmen.

Neben den internen bestehen aber auch externe IRT, welche Ihre Dienste in entsprechender Form der Privatwirtschaft anbieten und damit u.U. ein internes Incident Response Team ergänzen oder sogar ersetzen können. Eine wichtige Aufgabe eines IRT ist, im Sinne von Prävention und Frühwarnung, die aktuell vorhandenen Bedrohungen und Schwachstellen zu erkunden und wahrzunehmen, um möglichst frühzeitig Gegenmassnahmen zu ergreifen oder einzuleiten und damit ein Schadenereignis weitgehend zu verhindern oder Schäden lindern zu können. Erreicht ein Ereignis gewisse Kriterien so muss das IRT auch die Problemlösung an andere vorgegebene Organisationsstellen eskalieren. Als Informationsquellen zur Erkennung und Beurteilung von Incidents dienen interne Überwachungssysteme (z.B. Intrusion-Detection-Systeme) sowie externe „Computer Emergency Response Teams“ (CERTs), „Computer Security Incident Response Team“ (CSIRTs), Melde- und Analysestellen, Computer-Sicherheits-Laboratorien usw., über die ein fortlaufendes Incident Monitoring vorgenommen werden kann. Neben der Erkennung, Analyse und Bekämpfung der Incidents, kommt der Registrierung, Dokumentation und Berichterstattung der Vorfälle eine wichtige Bedeutung zu. Somit pflegt das Incident-Response-Team auch eine enge Zusammenarbeit mit dem IT-Service-Desk.