SCHUL-IT NAVIGATOR

Gefährdung nach BSI

Dargestellt ist eine Zusammenfassung der elementaren Gefährdungen für Zielobjekte im Bereich der IT, es sind dabei nicht alle Gefährdungen für jedes Zielobjekt relevant. So kann Wasser beispielsweise die Hardware-Komponenten an einem Standort beschädigen, bedroht aber nicht die Cloud-Lösungen mit denen die Hardware verbunden ist, sofern diese an einem anderen Ort gehostet wird.

G 0.1 Feuer

Direkte Schäden an Menschen, Gebäuden, Einrichtung. Folgeschäden durch Löschwasser, Rauch und Gase auch an nicht direkt vom Brand betroffenen Orten möglich.

G 0.2 Ungünstige klimatische Bedingungen

Hitze, Frost, Luftfeuchtigkeit und häufige Schwankungen der klimatischen Bedingungen können zu Schäden an Technik und der Arbeitsunfähigkeit, Verletzung oder dem Tod von Menschen führen.

G 0.3 Wasser

Wasser kann zu Schäden an technischen Komponenten führen. Mögliche Folgen sind Kurzschlüsse, mechanische Beschädigung, Rost und Frost.

G 0.4 Verschmutzung, Staub, Korrosion

Mechanische Komponenten sind störungsanfällig für geringe Mengen Staub und Verschmutzungen. Können zu Ausfällen oder Beschädigungen von IT-Komponenten und Versorgungseinrichtungen führen. Es gibt oft Sicherheitsschaltungen in den Geräten für ein rechtzeitiges Abschalten.

G 0.5 Naturkatastrophen

Naturkatastrophen können Beschädigungen an technischen Einrichtungen und Gebäuden hervorrufen sowie zu Verletzungen oder dem Tod von Menschen führen. Größe des Risikos ist stark Standort abhängig, betrifft auch den Ausfall von wichtigen Versorgungseinrichtungen.

G 0.6 Katastrophen im Umfeld

Gefahr durch Unglücksfälle mit Bränden, Explosionen, Freisetzung giftiger Substanzen oder Austreten gefährlicher Strahlung und den daran anschließenden Aktivitäten wie z. B. Sperrungen. Mögliche Gefahren aus dem Umfeld sind der Verkehr, Nachbarbetriebe oder Wohngebiete.

G 0.7 Großereignisse im Umfeld

Gefahr durch Behinderungen des ordnungsgemäßen Betriebs entsteht durch z. B. Straßenfeste, Konzerte, Sportveranstaltungen oder Demonstrationen. Zusätzliche Gefahren bei Ausschreitungen sind die Einschüchterung von Mitarbeitern und Gewaltanwendung gegen Personal oder Gebäude.

G 0.8 Ausfall oder Störung der Stromversorgung

Abschaltungen und Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber können bereits ab 10 ms den IT-Betrieb stören. Dies betrifft neben der IT auch Infrastruktur-Einrichtungen wie Aufzüge, Klimatechnik, Gefahrenmeldeanlagen und automatische Türschließanlagen.

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

Der Ausfall oder die Störung von Telefon, Fax, E-Mai oder dem Internet über einen längeren Zeitraum führt dazu, dass Geschäftsprozesse nicht mehr weiterbearbeitet werden können, Kunden die Institution nicht mehr erreichen können und Aufträge nicht abgegeben oder beendet werden können.

G 0.10 Ausfall oder Störung von Versorgungsnetzen

Ausfälle oder Störungen führen möglicherweise dazu, dass Personal nicht mehr arbeiten kann oder zu einer Beeinträchtigung des IT-Betriebs. Beispiele wichtiger Versorgungsnetze sind Strom, Telefon, Kühlung, Heizung bzw. Lüftung, Wasser und Abwasser, Löschwasserspeisungen und Melde- und Steueranlagen.

G 0.11 Ausfall oder Störung von Dienstleistern

Durch Ausfälle von externen Dienstleistungen kann die Aufgabenbewältigung und die betriebliche Kontinuität beeinträchtigt werden. Gleiches gilt für Unterauftragnehmer des Dienstleisters.

G 0.12 Elektromagnetische Störstrahlung

Elektronische Komponenten sind anfällig für elektromagnetische Störstrahlung. Folgen sind Ausfälle, Störungen, falsche Verarbeitungsergebnisse oder Kommunikationsfehler. Bei drahtloser Kommunikation sind die Frequenzbänder anfällig und bei Datenträgern können Informationen durch elektromagnetische Strahlung gelöscht oder verfälscht werden.

G 0.13 Abfangen kompromittierender Strahlung

Elektrische Geräte strahlen elektromagnetische Wellen ab, diese können Daten enthalten, die in näherer Umgebung abgefangen und rekonstruiert werden können. Auch Schallwellen haben das Risiko, abgefangen zu werden, um Informationen zu erlangen (z. B.von Druckern oder Tastaturen).

G 0.14 Ausspähen von Informationen (Spionage)

Wird u. a. genutzt, um Wettbewerbsvorteile zu erlangen, Personen zu erpressen oder ein Produkt nachbauen zu können. Mögliche Methoden sind technische, optische, akustische und elektronische. Daneben können auch öffentlich zugänglichen Quellen zusammengeführt werden.

G 0.15 Abhören

Ist eine Aufwand-Nutzen-Rechnung für die Angreifer. Die Methoden reichen vom Belauschen bis zum technischen Abfangen von Signalen. Das Entdeckungsrisiko ist gering und es gibt keine wirklich abhörsicheren Kabel, besonders gefährdet sind Klartextprotokolle wie HTTP.

G 0.16 Diebstahl von Geräten, Datenträgern, Dokumenten

Der Schaden besteht hier aus der Offenlegung vertraulicher Informationen, Kundenverlust und entstehenden Kosten für Wiederbeschaffung und Wiederherstellung eines arbeitsfähigen Zustandes. Betroffen sind u. a. Server, mobile Geräte und USB-Sticks.

G 0.17 Verlust von Geräten, Datenträgern, Dokumenten

Es entsteht ein Mangel an Verfügbarkeit, Kosten durch neu Beschaffung und es droht die Offenlegung von vertraulichen Informationen. Bei Wiederauftauchen besteht das Risiko, dass unerwünschte Programme aufgespielt wurden.

G 0.19 Offenlegung schützenswerter Informationen

Der Zugriff kann u. a. durch Diebstahl, unbedachte Weitergabe, unzureichende Vernichtung, Abhören oder Auslesen durch Schadprogramme erfolgen. Mögliche Folgen sind Gesetzesverstöße, negative Außen- und Innenwirkung und finanzieller Schaden.

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

Die Nutzung von Informationen und Produkten aus unzuverlässigen Quellen birgt das Risiko, dass falsche Daten als Basis für Entscheidungen oder Berechnungen genutzt werden. Außerdem ist dadurch die Integrität und Verfügbarkeit von IT-Systemen gefährdet.

G 0.4 Verschmutzung, Staub, Korrosion

Mechanische Komponenten sind störungsanfällig für geringe Mengen Staub und Verschmutzungen. Können zu Ausfällen oder Beschädigungen von IT-Komponenten und Versorgungseinrichtungen führen. Es gibt oft Sicherheitsschaltungen in den Geräten für ein rechtzeitiges Abschalten.

G 0.21 Manipulation von Hard- oder Software

Kann u. a. Geräte, Zubehör, Datenträger, Applikationen und Datenträger betreffen. Die Manipulation führt nicht immer zu unmittel-barem Schaden, je später entdeckt, desto größer ist oft der Schaden. Mögliche Schäden sind der Verlust von Vertraulichkeit, Integrität und Verfügbarkeit sowie die Zerstörung von Datenträgern oder IT-Systemen.

G 0.22 Manipulation von Informationen

Hier geht es um fehlerhaftes oder vorsätzlich falsches Erfassen oder Verändern von Daten. Wie schwerwiegend die Manipulation ist, ist abhängig von den Zugriffsmöglichkeiten, die eine Person auf Informationen hat.

G 0.23 Unbefugtes Eindringen in IT-Systeme

Jede Schnittstelle zu einem IT-System birgt das Risiko eines unbefugten Zugriffs.

G 0.24 Zerstörung von Geräten oder Datenträgern

Fahrlässigkeit, unsachgemäße Verwendung oder ungeschulten Umgang kann zu der Zerstörung von Geräten und Datenträgern führen. Damit geht auch die Gefahr einher, dass Informationen verloren gehen.

G 0.25 Ausfall von Geräten oder Systemen

Bei zeitkritischen Anwendungen sind die Folgeschäden nach einem Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

G 0.26 Fehlfunktionen von Geräten oder Systemen

Durch die Komplexität gibt es bei Soft- und Hardware viele unterschiedliche Fehlerquellen, die zu Fehlfunktionen und Sicherheitsproblemen führen können. Bleiben diese unentdeckt, kann dies zu Folgefehlern führen.

G 0.27 Ressourcenmangel

Der Mangel an personellen, zeitlichen, technischen und finanziellen Ressourcen kann zu Engpässen, Überlastungen und Ausfällen führen. Schon kleine Vorfälle können hier einen großen Impact auf die Geschäftsprozesse haben.

G 0.28 Software-Schwachstellen oder -Fehler

Wenn nicht rechtzeitig erkannt, können bei Anwendungen entstehende Abstürze oder Fehler zu weitreichenden Folgen führen, wie Fehler bei Berechnungsergebnissen, Fehlentscheidungen, Verzögerungen in Prozessen und Sicherheitslücken.

G 0.29 Verstoß gegen Gesetze oder Regelungen

Bei ungenügender Absicherung von Informationen, Prozessen und IT-Systemen kann es zu Verstößen gegen Rechtsvorschriften bei der Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern kommen. Bei mehreren Standorten gilt es ggf. unterschiedliche Gesetze zu beachten.

G 0.30 Unberechtigte Nutzung von Geräten oder Systemen

Bei IT-Systemen geht es hier insbesondere um die Identifikation und Authentisierung von berechtigten Benutzern. Die Folgen eines unberechtigten Zugriffs können Offenlegung von Informationen, Manipulationen und Störungen sein, insbesondere bei Administratorenrechten können schwere Schäden entstehen.

G 0.31 Fehlerhafte Nutzung von Geräten oder Systemen

Das Missachten oder Umgehen von Sicherheitsmaßnahmen kann zu Störungen oder Ausfällen führen. Bei fehlerhafter Bedienung von IT-Systemen oder Anwendungen können Daten versehentlich gelöscht oder verändert werden und vertrauliche Informationen an die Öffentlichkeit gelangen.

G 0.32 Missbrauch von Berechtigungen

Über Berechtigungen wird der Zugang zu Informationen gesteuert und kontrolliert. Oft verfügen Personen aus historischen, systemtechnischen oder anderen Gründen über umfangreichere Zutritts- oder Zugriffsrechte, als sie für ihre Tätigkeit benötigen, diese Rechte können für Angriffe missbraucht werden.

G 0.33 Personalausfall

Es wird unterschieden in unvorhersehbaren und vorhersehbaren Personalausfall. Beides kann Einfluss auf die Institution und die Geschäftsprozesse haben.

G 0.34 Anschlag

Diese Gefährdung kann für eine ganze Institution, bestimmte Bereiche oder einzelne Personen bestehen. Die Höhe des Risikos für eine Institution hängt von der Lage des Gebäudes, dem Aufgabenfeld und vom politisch-sozialen Klima ab. Für die Einschätzung der Bedrohung beraten auf Anfrage die Landeskriminalämter und das Bundeskriminalamt.

G 0.35 Nötigung, Erpressung oder Korruption

Nötigung oder Korruption können alle Grundwerte der Informationssicherheit beeinträchtigen. Ziele sind u. a. das Erlangen oder Manipulieren von Informationen oder die Störung von Geschäftsprozessen.

G 0.36 Identitätsdiebstahl

Hierfür werden personenbezogene Informationen wie Geburtsdatum, Anschrift, Kreditkarten- oder Kontonummern benötigt. Das Risiko ist bei geringer Identitätsprüfung in Verbindung mit teuren Dienstleistungen besonders hoch. Die Folgen bestehen oft aus Rufschädigung, finanziellem Schaden und einem hohen Zeitaufwand für die Aufklärung und Schadensbegrenzung.

G 0.37 Abstreiten von Handlungen

Neben Handlungen kann auch der Versandt oder Empfang von Informationen verleugnet werden. Gründe hierfür sind u. a. der Verstoß gegen Anweisungen, Sicherheitsvorgaben und Gesetze oder das Vergessen eines Termins. Im Bereich der Informationssicherheit wird häufig die Verbindlichkeit betont um sicherzustellen, dass erfolgte Handlungen nicht unberechtigt abgestritten werden können.

G 0.38 Missbrauch personenbezogener Daten

Der Missbrauch kann zu der Beeinträchtigung der gesellschaftlichen Stellung oder den wirtschaftlichen Verhältnissen einer Person führen. Ein Missbrauch liegt z. B. vor, wenn zu viele Daten gesammelt werden, es keine Einwilligung gibt, die Daten nicht rechtzeitig gelöscht oder zweckentfremdet werden.

G 0.39 Schadprogramme

Es handelt sich dabei um Software, die ohne Wissen oder Einwilligung des Nutzers schädliche Funktionen ausführt. Die Möglichkeiten reichen von der Datenauslese bis zur Systemfernsteuerung. Der Schaden besteht aus dem Verlust oder der Verfälschung von Informationen,einem Imageverlust und finanziellem Schaden.

G 0.40 Verhinderung von Diensten

Angriffsformen (auch DoS-Angriff genannt) mit dem Ziel, die vorgesehene Nutzung von Dienstleistungen, Funktionen oder Geräte zu verhindern, z. B. durch das verursachen von IT-Ausfällen. Dabei werden meistens die Ressourcen einer Institution durch den Angreifer überbeansprucht, damit sie für die eigentlichen Nutzer nicht mehr zugänglich sind.

G 0.41 Sabotage

Diese mutwillige Manipulation oder Beschädigung von Sachen oder Prozessen erfolgt überwiegend durch interne Täter. Häufige Ziele sind Rechenzentren oder Kommunikationsanbindungen, diese werden insbesondere über unzureichend geschütze Infrastruktur punktuell manipuliert.

G 0.42 Social Engineering

Hierbei werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Eine oft genutzte Methode sind Telefonanrufe unter Vortäuschung falscher Autorität oder Zugehörigkeit, um Passwörter o. Ä. zu erlangen. Auch mehrstufige Angriffe über einen längeren Zeitraum sind möglich.

G 0.43 Einspielen von Nachrichten

Angreifer senden speziell vorbereitete Nachrichten mit dem Ziel, für sich selbst einen Vorteil oder einen Schaden für das Opfer zu erreichen. Für die Konstruktion werden z. B. Protokollspezifikationen oder Aufzeichnungen über das Kommunikationsverhalten in der Vergangenheit genutzt.

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Mit dem Eindringen einhergehende Gefahren sind Diebstahl und Manipulation von Informationen oder IT-Systemen. Daneben sind Sachschäden an Eingängen und Geräten möglich.

G 0.45 Datenverlust

Häufig werden Daten unbeabsichtigt oder unerlaubt gelöscht, z. B. durch Fehlbedienung, Fehlfunktionen, Stromausfälle, Verschmutzung oder Schadsoftware. Ein Datenverlust kann jedoch auch durch Beschädigung und Diebstahl von Geräten oder Datenträgern entstehen oder durch Unachtsamkeit bei der Synchronisierung von Geräten.

G 0.46 Integritätsverlust schützenswerter Informationen

Mögliche Folgen des Integritätsverlustes sind, dass Informationen nicht mehr lesbar sind oder entschlüsselt werden können. Verfälschte Daten führen dazu, dass falsche Informationen weitergegeben werden und elektronischen Dokumente verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.

G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

Diese Seiteneffekte treten aufgrund der hohen Komplexität und Vernetzung moderner Informationstechnik auf und können von den Tätern unbeabsichtigt sein, andere Objekte betreffen oder Unbeteiligte schädigen.

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html