Kuratorium Sicheres Österreich Cyber-Risikomatrix

Glossar

20.09.2011

Bösartige Software	Programme, die schadhafte Funktionen ausführen (Viren, Trojaner, Malware, Würmer). Dieser Schadcode kann Systeme, Netzwerke, Anwendungen oder einzelne Dateien unbrauchbar machen, sich eigenständig auf andere Netzwerke verbreiten und zu ungewünschten Aktivitäten verleiten. In SCADA-Umgebungen kann Malware die gesamte Steuerungs- und Regelfähigkeit von Industrieanlagen aufheben oder Fernzugriffe einrichten.	Eigentümerstruktur kritischer IKT-Infrastruktur	Veränderungen in der Eigentümerstruktur der strategisch bedeutenden IKT-Infrastrukturen können ein Risiko für die öffentliche Ordnung und Sicherheit darstellen, wenn neue Eigentümer mit entsprechendem Stimmen- und Kapitalanteil z.B. die personelle Besetzung der Führungsgremien verändern oder Einfluss auf die Geschäftsstrategie des entsprechenden Unternehmens nehmen.
Cybercrime	Jede Form von Straftaten, die mit Hilfe von Informationstechnologien und Kommunikationsnetzen begangen werden. Auch die Internetkriminalität zählt dazu.	Fahrlässiges Verhalten bei strategischen Infrastrukturbetreibern	Fahrlässiges Nutzerverhalten (unsichere Passwörter, Öffnen von Spam-eMails, etc.) stellt immer noch die größte Gefährdung für IT-Systeme dar. Umso mehr ist dieses Verhalten bei strategischen Infrastrukturbetrieben problematisch und muss gezielt durch Schulungs- und Auditmaßnahmen verhindert werden.
Cyberspionage	Spionage auf digitalem Weg, um Informationen aus elektronischen Datenbanken staatlicher Behörden und wissenschaftlicher Institute zu gewinnen, aufzuklären, wie diese miteinander kommunizieren oder Innenansichten über die Position eines Staates zu Sachfragen zu gewinnen.	Fehlende bzw. nicht aktuelle, rechtliche Grundlagen	Rechtliche Regulierungen sind derzeit noch primär auf Datenschutz und nicht gesamtheitlich auf IT-Sicherheit fokussiert.
Cyberspionage gegen Industrie	Spionage auf digitalem Weg gegen Unternehmen, die damit Werte, Knowhow und Ansehen oder durch Erpressung die Existenz verlieren können.	Fehlende, strategische Netzwerkstrukturplanung	Die schnell wachsende Nachfrage nach Übertragungskapazitäten in den unterschiedlichsten Formen sowie die damit zusammenhängende Notwendigkeit der Steuerung und Verwaltung dieser Übertragungskapazitäten stellt neue Anforderungen an die Netzwerkstrukturplanung. Ohne eine strategische Planung der Entwicklung der Übertragungsnetzwerke (z.B. welche Kapazitäten werden bereitgestellt, welche Anschlüsse erfolgen wann und wo?) besteht das Risiko, dass diese den Anforderungen nicht Stand halten und sich dadurch die Anfälligkeit für unbeabsichtigte und beabsichtigte Störungen erhöht.
Cyberterrorismus	Dabei handelt es sich um organisierte Cybersabotage/-angriffe, die von politisch-fundamentalistischen bzw. terroristischen Gruppen oder Einzeltätern organisiert werden und sich gegen Staaten, Organisationen oder Unternehmen richten.	Fehlender Regulierungsfokus auf IKT-Sicherheit	National und international gibt es verschiedene Standards zur Förderung der Unternehmenssicherheit im Allgemeinen und des Schutzes der strategisch bedeutenden Infrastrukturen im Besonderen. Das Risiko besteht darin, dass Standards für die IKT-Sicherheit noch zu sehr aus einer sektorspezifischen Sichtweise definiert werden, womit der Blick für den Querschnittscharakter dieses wichtigen Aufgabenbereichs verloren geht. Daraus resultiert die Gefahr uneinheitlicher Anforderungen an die IKT-Sicherheit in unterschiedlichen strategisch bedeutenden Infrastruktursektoren.
Cyberwar	Meint die kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus dem Bereich der Informationstechnik. In einem weiteren Sinne ist damit auch die Unterstützung militärischer Aktionen in den klassischen Operationsräumen Boden, See, Luft, Weltraum durch Maßnahmen aus dem virtuellen Raum angesprochen. Ganz allgemein werden darunter auch die hochtechnisierten Formen des Krieges im Informationszeitalter gemeint, die auf einer weitgehenden Computerisierung, Elektronisierung und Vernetzung fast aller militärischer Bereiche und Belange basieren.	Fehlendes Fachpersonal	Fehlendes oder nicht richtig ausgebildetes Fachpersonal kann die negativen Folgen bestehender, technischer Schwächen zusätzlich verstärken.
Datendiebstahl und Manipulation von Bürgerdaten	Die öffentliche Verwaltung benötigt digitale Informationen zu den Bürgern, die in verteilten oder zentralen Datenbanken gespeichert sind. Ein Diebstahl oder eine Manipulation der Bürgerdaten würde das Vertrauen der Bürger und der staatlichen Institutionen in die über die Bürger gespeicherten Daten verletzen. Eine eindeutige Identitätsfeststellung und die Zuordnung von Rechten und Pflichten der Bürger wäre damit schwierig bis unmöglich.	Fehlendes oder unzureichendes BCM	Business Continuity Management (BCM) dient der Vorbereitung von Behörden und Unternehmen zur Bewältigung von Schadensereignissen. Ziel ist, dass die jeweilige Organisation möglichst schnell ihren Normalbetrieb wieder aufnehmen kann. Aufgrund der zunehmenden Vernetzung zwischen den Unternehmen und den strategisch bedeutenden Infrastruktursektoren besteht die große Herausforderung darin, BCM verstärkt organisationsübergreifend anzulegen. Das ist gegenwärtig oft noch nicht der Fall, so dass die Organisationen an den Schnittstellen zu ihren Drittlieferanten (Service Level Agreement) verwundbar sind.

Fehlerhafte, inkompatible Codes/Software	Programme bestehen aus hundertausenden bis Millionen Zeilen langen Codes. Bei der Entwicklung können sich Fehler eingeschlichen haben in Bezug auf Verfügbarkeit, Funktion oder Sicherheit. Durch ständige Weiterentwicklung passen verschiedene Programme und Prozesse in der verwendeten Software oft nicht mehr korrekt zusammen, sie sind also inkompatibel. Es besteht die Gefahr, durch solche Fehler und Inkompatibiltäten handlungsunfähig zu werden, Wissen zu verlieren oder nur mit extremen Aufwand Systeme wieder zum Laufen zu bringen.	Manipulation der IKT-Systeme der Energieerzeugung und -versorgung	Durch Störungen der SCADA-Systeme und Einbruch in die zentralen Verteilersysteme können Ausfälle herbeigeführt, Übertragungen gestört und die Erzeugung von Energie erheblich erschwert, wenn nicht sogar unmöglich gemacht werden. In Rechenzentren stellen Spannungsschwankungen, Spannungsspitzen sowie kurzer und längerer Stromausfall eine reale Bedrohung dar.
Geknackte, digitale Schlüsselsysteme	Sichere Kommunikation im Internet basiert auf Verschlüsselungstechniken, die auf dem Prinzip beruhen, dass die Entschlüsselung einer geschützten Information ohne Kenntnis eines geheimen Schlüssels unmöglich und ein Ausprobieren von möglichen Schlüsseln zu aufwändig ist. Diese Sicherheit baut auf mathematischen Verfahren auf, für die keine einfachen Lösungen bekannt sind. Sollte eine mathematische Lösung für eines dieser Verschlüsselungsverfahren gefunden werden, könnte das Verfahren schlagartig nicht mehr für die Absicherung der Internetkommunikation benutzt werden. Eine Umstellung der gängigen Verfahren würde aber nur mit sehr hohem Aufwand durchführbar sein.	Manipulation der IKT-Systeme des Verkehrssektors	Im Verkehrssektor werden IKT-Systeme zur Steuerung des Verkehrsflusses (Verkehrsmanagement) und zum Betrieb der einzelnen Plattformen (z.B. Autos, Bahn, Schiffe, Flugzeuge) verwendet. Cyber-Risiken können sich unkontrolliert verbreiten, denn die Netze sind durch den Einsatz von IKT miteinander verbunden und voneinander abhängig. Die Cyber-Sicherheit von Verkehrsleitsystemen kann zum Beispiel durch Malware gefährdet werden; ebenso besteht die Möglichkeit, dass Verkehrsleitsysteme durch das Einschleusen von Trojanern ferngesteuert werden. Die Folgen sind bewusst angerichtetes Chaos im Verkehrssektor.
Kein Sicherheitsgütesiegel/Audits	Sicherheitsüberprüfungsstandards und Audits existieren, werden aber nur bei wenigen Zielgruppen (z.B. Smartcards) oder nur auf freiwilliger Basis (z.B. ISO 27001) durchgeführt. Ein einheitliches Sicherheitsgütesiegel und verstärkt durchgeführte Audits würden es den Anwendern erleichtern, eine Entscheidung betreffend der Sicherheit eines Produktes oder Betriebes zu treffen.	Manipulation der IKT-Systeme des Zahlungsverkehrs und der Finanztransaktionen	Der finanzielle Zahlungsverkehr ist für die reibungslose Funktion einer Volkswirtschaft von essentieller Bedeutung. Nicht nur der Bürger wickelt seinen Zahlungsverkehr elektronisch per Kreditkarte oder e-Banking ab; gleiches gilt auch für die Geschäftsbanken und den Verkehr zwischen den Nationalbanken. Die bewusste oder zufällige Störung der elektronischen Systeme, die hierfür eingesetzt werden, kann die Liquiditätsversorgung Österreichs nachhaltig beeinflussen. Aufgrund der engen Verflechtung der nationalen Bankensysteme sind internationale Auswirkungen nationaler Liquiditätsengpässe nicht auszuschließen.
Keine systematische Technologiefolgenabschätzung	Neue Technologien werden durch entsprechenden Marktdruck und durch das Versprechen, aktuelle Probleme zu lösen, so rasch als möglich eingeführt. Eine Abschätzung von langfristigen Technologiefolgen entfällt oder wird nicht systematisch und für alle wesentlichen Technologien durchgeführt.	Manipulation der IKT-Systeme für Cloud-Services	Cloud-Services werden in drei Delivery Modelle unterteilt: Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service. Es besteht keine Möglichkeit, tatsächlich festzustellen, wo sich die Daten physikalisch befinden, wer darauf Zugriff hat, wie diese Daten abgesichert sind und ob die lokalen Datenschutzbestimmungen den eigenen Erwartungen entsprechen.
Lückenhafte Cybergovernance	Das Fehlen von Konzepten, Verfahren und Gremien/Plattformen für die öffentlich-private, öffentlich-öffentliche und private-private Zusammenarbeit im Kontext der Cybersicherheit ist ein Risiko, weil staatliche und private Maßnahmen dadurch nicht gut genug aufeinander abgestimmt werden können. Lücken und möglicherweise auch widersprüchliche Maßnahmen können die Folgen davon sein.	Manipulation der IKT-Systeme in der Wasserwirtschaft	Damit ist eine Manipulation der Gesamtheit der Systeme für die Bereitsstellung von Trinkwasser, Prozess/Brauchwasser und die Entsorgung bzw. Wiederaufbereitung von Abwasser gemeint. Die Steuerungselemente (SCADA), die für Wassermanagementsysteme verwendet werden, sind für absichtliche Störungen/Manipulationen anfällig, was die Versorgung mit Wasser beeinträchtigen kann.
Macht der sozialen Netze und deren Manipulation	Soziale Netze können gezielt manipuliert werden, um die öffentliche Meinung zu beeinflussen und Falschmeldungen zu verbreiten.	Manipulation von GPS (Zeitsynchronisation)	Über GPS beziehen viele IKT-Systeme eine hochgenaue Uhrzeit für synchronen Betrieb mit anderen Systemen, Logbucheinträge, Start und Stopp von Prozessen, etc.
Mangelnde Sicherheitsstandards/bewusst-sein im Gesundheitswesen	IKT-Systeme im Gesundheitswesen reichen von den Datenverarbeitungssystemen zur Speicherung der Patientendaten, über telemedizinische Anwendungen und technische Geräte, die für Operationen, die Überwachung und die Steuerung von Lebensfunktionen wichtig sind, bis hin zu Anwendungen, die älter werdende Menschen im Alltag unterstützen (Ambient Assisted Living). Aus der Möglichkeit, diese Systeme zu manipulieren, resultieren unterschiedliche Risiken wie z.B. der Missbrauch von Patientendaten oder die bewusste Störung lebenserhaltender Geräte (z.B. Hacking von Herzschrittmachern oder Insulinpumpen).	Manipulation von Kommunikations- und SAT-Verbindungen	Beinhaltet die Manipulation aller möglichen Kommunikationsverbindungen, die zur Daten- (z.B. Internet) und Sprachverbindung notwendig sind. Eine Manipulation der Verbindungen kann durch Umleitung, Unterbrechung, Abhören und Einschleusen fehlerhafter bis bösartiger Informationen erfolgen.

Manipulierte bzw. unsichere Hardware	Hardware wird zur Kostenoptimierung und ohne Kontrollmöglichkeit für den Kunden verteilt auf mehrere Länder entwickelt und im Massenprozessen hergestellt. Detaillierte Prüfungen der Hardware auf Manipulationen (z.B. Abhöreinrichtungen in Bankomat-Kassenterminals) oder Unsicherheiten (Öffnen von WLAN-Verbindungen ohne, dass dies konfiguriert wurde) können nur selten durchgeführt werden. Und auch die geprüfte Sicherheit eines Testexemplares garantiert nicht, dass nicht andere Exemplare der Hardware manipuliert oder unsicher sind.	Unzureichendes Cyberlagebewusststein/-verständnis	Fehlendes Lagebewusstsein und Lageverständnis bezüglich der Vorgänge im Cyberspace führen dazu, dass die handelnden Akteure die Gefahren und deren mögliche Folgen nicht oder nicht rechtzeitig erkennen und damit unterschätzen. Negative Folgen können sein: unzureichende Vorbereitung, keine oder nicht ausreichende Abwehr- und Bewältigungsmaßnahmen/-mittel sowie mangelhafte Fähigkeiten zur Wiederherstellung des Normalbetriebs.
Nicht erkannte (IKT-)Anomalien	Anomalien beschreiben unerkannte und unbekannte Schwachstellen, Funktionen und Wirkungen von Hard- und Software sowie den zugrundliegenden Protokollen, so dass es schwierig ist, dagegen frühzeitig entsprechende Massnahmen (z.B. Erkennen, Abwehr, Wiederherstellen) zu ergreifen.	Verletzlichkeit der IKT-Infrastruktur durch Naturkatastrophen	IKT-Infrastruktur kann durch massive Naturkatastrophen (Hochwasser, Erdbeben, etc.) beschädigt oder unerreichbar werden.
Social Engineering	Im Zusammenhang mit IT-Sicherheit wird der Begriff für eine Strategie von Online-Betrügern gebraucht. Indem sie individuell auf ihre Opfer zugehen, steigern sie ihre Erfolgsraten: zuvor ausspionierte Daten wie etwa die Surfgewohnheiten oder Namen aus dem persönlichen Umfeld des Opfers werden dafür verwendet, bespielsweise Phishing-eMails persönlich zu formulieren und dadurch Vertrauen zu wecken.	Verteilte Angriffe auf Systeme (DDOS)	„Distributed Denial of Service“: Angriffe, bei denen eine große Anzahl an Computern verwendet wird, um ein bestimmtes Computersystem durch eine hohe Anzahl an Anfragen zu blockieren.
Systematischer Diebstahl digitaler Identitäten	Eine digitale Identität ist die Teilmenge der Attribute einer Entität, welche diese Identität in einem bestimmten Kontext im Unterschied zu anderen Entitäten bestimmbar machen. Eine Entität kann abhängig vom Kontext und den dadurch erforderlichen Attributen auch mehrere, digitale Identitäten besitzen. Das von organisierten Gruppen oder Einzeltätern durch Trojaner ermöglichte Ausspähen und Nutzen von fremden ID-Attributen stellt eine sehr hohe Bedrohung dar.		
Ungenügender Anreiz für Sicherheitsinvestitionen	Der Regulierungsfokus der meisten Länder, die staatliche Leistungen durch die Liberalisierung den Kräften des Marktes überlassen haben, liegt auf der Kostenseite. Durch die Liberalisierung sollen die Konsumenten von niedrigeren Preisen profitieren. Beispiele aus unterschiedlichen Infrastruktursektoren (z.B. Eisenbahn) zeigen aber, dass ein einseitiger Kosten-/Preisfokus nicht nur die Qualität der Leistungen, sondern auch deren Sicherheit beeinträchtigen kann. Sicherheitsinvestitionen stellen für Unternehmen direkte Kosten dar. Fehlen die Anreize für solche Investitionen, erfolgen sie in der Regel nicht.		
Unklare Kompetenzlage der Behörden	Unklare Aufgabenverteilungen und Zuständigkeiten der Behörden für Cyber-Risiken. Teilweise mehrfache Abdeckung von bestimmten Cyber-Risiken durch mehrere Ministerien und Behörden.		
Unsichere Steuerungssysteme (z.B. SCADA)	Industrielle Steuerungssysteme sind weit verbreitet und steuern und messen unzählige Produktionsprozesse. Die Verbreitung des Stuxnet-Wurms (der iranische Nuklearanlagen befallen hat) hat gezeigt, dass diese Systeme anfällig für Sicherheitsprobleme sind und deaktiviert, zerstört oder ferngesteuert werden können.		