asut Position

5G-Cybersicherheit in der Schweiz

Bern, März 2021

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

@asut_ch

Inhaltsverzeichnis

1. Einleitung

Die neue Mobilfunkgeneration 5G wird seit 2019 in der Schweiz eingeführt. Sie ist effizienter als bisherige Mobilfunktechnologien, bietet neue und bessere Funktionalitäten und wurde u. a. im Hinblick auf das Internet der Dinge konzipiert. Aufgrund der Leistungsfähigkeit, der höheren Effizienz und der universellen Einsatzmöglichkeiten gilt 5G als eigentliche Basistechnologie für die Digitalisierung von Wirtschaft und Gesellschaft.

Mit der zunehmenden Vernetzung und Digitalisierung bekommt die Cybersicherheit eine wichtigere Bedeutung. Dies gilt grundsätzlich für alle Informations- und Kommunikationstechnologien (IKT) und nicht nur für 5G. Der Schweizerische Verband der Telekommunikation (asut) engagiert sich deshalb in der Fachkommission Cyber-Security von DigitalSwitzerland gemeinsam mit anderen Verbänden sowie Behörden und Unternehmen für die «Härtung» der IKT in der Schweiz.

In den letzten zwei Jahren wurde 5G Gegenstand eines politischen Schlagabtausches zwischen den USA und China. Im Zentrum standen Vorwürfe, dass chinesische Unternehmen 5G im Auftrag staatlicher Behörden für Cyberattacken, beispielsweise zur Spionage, einsetzen könnten. Damit verbunden stellt sich die Frage, ob 5G sicher ist oder nicht.

asut hat dazu innerhalb des Verbandes Sicherheitsexperten befragt und das vorliegende Positionspapier zur 5G-Cybersicherheit erstellt. Darin wird aufgezeigt, wie sich 5G von anderen Mobilfunk-Technologien unterscheidet und welche Massnahmen ergriffen werden können und sollen, um die Cybersicherheit in 5G-Netzen sicherzustellen.

Das Positionspapier konzentriert sich auf die Technik (z. B. Standards) und auf die Mobilfunkbetreiber in der Schweiz. Dazu gehören auch Fragen zur Sicherstellung der Cybersicherheit über die Lieferkette (Supply Chain). Damit wird der Situation Rechnung getragen, dass Telekommunikationsnetze aus einer Vielzahl von Komponenten unterschiedlicher und meist internationaler Lieferanten bestehen.

Nicht behandelt werden hingegen Aspekte des verbotenen Nachrichtendienstes in der Schweiz oder die Rechtslage in den Herkunftsländern von Lieferanten betreffend Kooperation mit staatlichen Stellen. asut verfügt dazu weder über konkrete Informationen noch über das Know-how, diese Aspekte zu analysieren und zu bewerten.

Offen bleibt zudem das Themenfeld der 5G-Anwendungen ausserhalb der Telekommunikations-Branche. Fragen zu IoT-Anwendungen wie vernetzten Fahrzeugen, Geräten etc. werden in einem nächsten Schritt angegangen.

2. Ausgangslage

Sicherheit im Betrieb

Die Gewährleistung der Sicherheit in Telekommunikationsnetzen ist seit Jahren eine zentrale Aufgabe der Telekomanbieter. Die hierzu notwendigen Vorkehrungen und Massnahmen wurden mit der Einführung jeder neuen Kommunikationstechnologie den jeweiligen Gegebenheiten angepasst. Dies gilt auch für die Einführung von 5G.

Einige zentrale Anforderungen bezüglich Sicherheit sind in der Schweiz durch rechtliche Grundlagen (Datenschutzgesetz, Fernmeldegesetz, Verordnung über Fernmeldedienste etc.) festgeschrieben. Diese Regularien haben sich aus Sicht der Telekommunikationsbranche bewährt, da sie eine der Unternehmenssituation angepasste Umsetzung von Security-Massnahmen erlauben.

Um Privat- und Geschäftskunden zu schützen, geben sich die Betreiber in Eigenverantwortung strikte Sicherheitsregimes und bauen dazu eigene Sicherheitsorganisationen auf. Zu den wichtigsten Massnahmen gehören etwa:

- Der Betrieb eines Informations-Sicherheits-Managementsystems (ISMS) nach ISO 27001
- Der Betrieb eines Security Operation Centers (SOC) oder einer vergleichbaren Instanz, also einer zentralen Organisation, die die Sicherheit im Netz ständig überwacht, Bedrohungen analysiert und Massnahmen ergreift respektive veranlasst.
- Das Pflegen eines Business Continuity Managements (BCM), um den Betrieb von systemkritischen Prozessen zu schützen und im Krisenfall aufrecht zu erhalten.
- Penetrationstests (Pentests), mit denen untersucht wird, ob Angreifer mit bekannten Methoden unautorisiert in das Netz eindringen können.
- Leakage Prevention, also die Verhinderung respektive Detektion von nicht-autorisierten Datenabflüssen.

Sicherheit im Betrieb ist eine der Grundvoraussetzung für das Geschäft in der Telekommunikation. Deshalb gehen die Betreiber das Thema sehr gründlich und systematisch an. Weil die Implementation von Funktionen, Schnittstellen etc. den jeweiligen Betreibern überlassen ist, kann es für die Sicherheit aber keine Einheitslösung geben. Vielmehr wird je nach Ausgangslage und Rahmenbedingungen auf die geeigneten Standards und Best-Practice-Empfehlungen zurückgegriffen. Am Ende richten sich die jeweiligen Sicherheitskonzepte nach den angebotenen Diensten, den Eigenheiten der Netze und Infrastrukturen, den technischen Rahmenbedingungen, der jeweiligen Bedrohungslage sowie natürlich den Bedürfnissen der Kunden.

Sicherheit in der Lieferkette

Auch die Sicherheit der Lieferkette ist kein 5G-spezifisches Thema. Sie wird von den Betreibern und von den Herstellern der Telekomunikations-Systeme bereits heute konsequent berücksichtigt. Dabei umfassen die Lieferanten nicht nur den direkten Technologiepartner der Telekommunikationsanbieter, sondern letztlich die ganze Lieferkette für die Herstellung aller Komponenten. Angesichts der Bedeutung, die 5G-Netze dereinst für den Betrieb auch von kritischen Infrastrukturen haben sollen, erhält die Frage der Sicherheit in der Lieferkette aber zusätzliches Gewicht. Zu unterscheiden sind zwei Arten von Bedrohungen:

Fehler oder Schwachstellen in der Ausrüstung: Die höhere Komplexität von 5G-Netzen sowie ihre grössere Abhängigkeit von Software und Diensten von Drittanbietern erhöhen die Risiken durch Schwachstellen. Solche Schwachstellen und Hintertüren können entweder be-

reits in den gelieferten Geräten vorhanden sein oder erst im Lauf der Zeit durch Softwareupdates eingebracht respektive aktiviert werden. Schwachstellen dieser Art sind bereits heute eine Hauptursache für gravierende und lang andauernde Angriffe auf Netzwerke aller Art.

Grund für Schwachstellen bei der Software ist meist ein mangelhaftes Qualitätsmanagement bei der Software-Entwicklung. Minderwertige Produktqualität kann auch entstehen, wenn die relevanten Standards bei der Herstellung nicht eingehalten werden oder standardisierte Sicherheitsfunktionen nicht implementiert wurden. Als weitere Ursache kommen absichtlich durch den Lieferanten oder Dritte eingebaute Schwachstellen infrage. Sie können etwa dazu gebraucht werden, ein Netz oder Teile davon zu manipulieren. Solche Manipulationen können auch im Auftrag eines Staates entweder durch den Lieferanten oder durch eine andere Organisation, wie etwa einen Geheimdienst, durchgeführt werden. Konkret sind folgende Szenarien denkbar:

- Sabotage, etwa durch den Einbau von Funktionen, mit denen sich ganze Netze oder Teile davon in der Funktion beeinträchtigen lassen
- Spionage via eingebauter Backdoors, durch die Daten ausgeleitet werden

Was die Sicherung der Lieferkette angeht, bedienen sich die Schweizer Betreiber geeigneter und erprobter Instrumente. Hierzu gehören unter anderem internationale Standards und Normen wie ISO 28000. Im Gegensatz zu den technischen Risiken in der Lieferkette entzieht sich die Bedrohung durch Fremdstaaten oder spezialisierte Organisationen aber dem Einfluss der Betreiber.

Abhängigkeit von einem einzelnen Lieferanten: Ist ein Betreiber von einem bestimmten Lieferanten vollständig abhängig, kann dies zu weiteren Schwachstellen führen. So kann der fehlende Wettbewerbsdruck zur Folge haben, dass bekannte Sicherheitslücken nicht umgehend behoben werden. Dadurch könnten Schwachstellen ausgenutzt werden (exploited). Denkbar ist auch, dass die Lieferkette infolge der Abhängigkeit von einem einzigen Lieferanten unterbrochen wird. Dies könnte beispielsweise infolge von politisch motivierten Massnahmen (Handelskonflikt) oder bei Lieferengpässen aufgrund einer Pandemie eintreten – mit entsprechenden Folgen für den Betrieb von 5G-Netzen oder sonstigen Telekommunikationsnetzen. Besonders gravierend wäre dieses Risiko, wenn ein Lieferant eine dominante Position für ein ganzes Land hat.

In der Schweiz hat der Infrastrukturwettbewerb gemäss Fernmeldegesetz dazu geführt, dass die grossen Telekommunikationsanbieter 5G-Technik von verschiedenen Systemlieferanten einsetzen. Das reduziert das Ausfallrisiko bereits deutlich. Betriebsrelevante Risiken aus der Lieferkette werden zudem durch adäquates Business Continuity Management (BCM) angegangen. Hierfür liefert beispielsweise die Norm ISO 20243 die entsprechenden Anforderungen und Konzepte. Das einschlägige Instrumentarium wird ständig weiterentwickelt und sorgt bereits heute für Sicherheit in der Lieferkette.

3. Neuerungen bei 5G-Netzen

Zusätzliche Sicherheitsfunktionen

Technisch gesehen ist 5G deutlich stärker auf Sicherheit ausgelegt als die Vorgänger-Technologien. Zu den neuen Errungenschaften gegenüber 3G/4G gehören insbesondere:

- Der striktere Authentifizierungsprozess beim Anmelden am Funknetz
- Die stärkere und konsequentere Verschlüsselung der Daten
- Die Sicherung und Trennung der Komponenten im Netz mit neuen kryptografischen Lösungen. Sollten einzelne Komponenten angegriffen werden, ist der Schutz anderer Komponenten weiterhin gewährleistet.

- Die verschlüsselte Übertragung der Langzeitidentität der Teilnehmer (IMSI), wodurch Man-in-the-Middle-Attacken (siehe Anhang) mithilfe von IMSI Catchern nahezu verunmöglicht werden.
- Die Authentication Confirmation (AC) beim Roaming; dabei sendet das Gerät eines Nutzers einen kryptografischen Beweis über die Identität des Mobilfunkbetreibers, in dessen Netzwerk sich das Gerät eingewählt hat, zurück an den heimischen Mobilfunkbetreiber. Dieser verifiziert die Identität des Geräts und des ausländischen Netzes.

Diese und weitere Mechanismen werden dafür sorgen, dass 5G-Netze im Endausbau deutlich sicherer sein werden als ihre Vorgänger. Weil die 5G-Technik phasenweise eingeführt wird und 3G/4G für längere Zeit parallel betrieben werden, hängt es vom Migrationskonzept des Betreibers ab, wie rasch das volle Sicherheitspotenzial ausgeschöpft werden kann.

Sicherheitsrelevante technische Neuerungen

Neben den neuen Sicherheitsfunktionen bringt die fünfte Mobilfunkgeneration auch Veränderungen, die möglicherweise mit neuen Risiken verbunden sein können. Auf der einen Seite hängt das mit der Nutzung zusammen. So ist beispielsweise zu erwarten, dass die Anzahl der verbundenen Geräte massiv steigen wird, was die verwundbare Oberfläche der Netze vergrössert. Vorauszusehen ist auch, dass künftig vermehrt systemrelevante Infrastrukturen (Energie, Wasser, Verkehr etc.) oder unternehmenskritische Prozesse die 5G-Netze nutzen werden. Dies wiederum kann die Auswirkungen von Angriffen erhöhen.

Auf der anderen Seite ist 5G mit technischen Errungenschaften verbunden, die Auswirkungen auf die Sicherheit haben können. Im Wesentlichen sind hier zu nennen:

Software Defined Networks und Virtualisierung: Im Vergleich zu 3G/4G basiert 5G viel stärker auf Software. In diesem Zusammenhang hervorzuheben sind insbesondere der forcierte Einsatz von Software Defined Networks (SDN) und von Network Functions Virtualisation (NFV). Beide technischen Konzepte wurden schon früher in der Telekommunikation eingeführt. Aber erst bei 5G spielen sie eine zentrale Rolle – mit all ihren Vorteilen bezüglich Flexibilität, Erweiterbarkeit, Leistung und Funktionalität. Für die Sicherheit kann dies vorteilhaft sein, weil etwa Schwachstellen durch Aufspielen von Softwareaktualisierungen behoben werden können und nicht in die Hardware eingegriffen werden muss. Gleichzeitig steigt damit aber auch die Bedeutung von Drittanbietern, die solche Updates in der notwendigen Frequenz und Qualität bereitstellen müssen.

Hinzu kommt, dass mangelhaftes Sicherheitsmanagement bei der Softwareentwicklung ausgenützt werden könnte, um beispielsweise böswillig Hintertüren (Backdoors) in die Produkte einzubauen. Solche Manipulationen lassen sich von den Betreibern im Nachhinein schwer entdecken, zudem können sie sehr gravierende Auswirkungen haben. Hier braucht es also nicht nur ein robustes Patch-Management, sondern auch eine wirksame Überwachung und Sicherung der Lieferkette.

Exkurs: Lawful Interception und Backdoors

Lawful Interception (LI) umfasst den Zugang zu den Fernmeldenetzen im Rahmen der Überwachung des Post- und Fernmeldeverkehrs. Dazu sind definierte Schnittstellen in den Systemen der Betreiber vorgesehen. Diese Schnittstellen sind gesetzlich vorgeschrieben und stellen keine Backdoors zu den Systemen dar. Die LI-Schnittstellen werden von spezialisierten Teams der Betreiber überwacht und dürfen nur im Auftrag der Strafverfolgungsbehörden genutzt werden. Die rechtlichen Grundlagen dazu finden sich im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und den dazugehörigen Verordnungen.

Internet-Technik: Im Unterschied zu seinen Vorgängern, baut 5G weitgehend auf Internet-Protokollen und weniger auf Telekom-spezifischen Protokollen auf. Aus Perspektive der Sicherheit hat das auf der einen Seite den Nachteil, dass Angreifern das breite Spektrum an internetbasierten Angriffsmethoden zur Verfügung steht. Sie müssen sich also nicht zuerst mit den Eigenheiten von Kommunikationsnetzen auseinandersetzen. Auf der anderen Seite sind diese Angriffsmethoden besser bekannt und es gibt bewährte Konzepte und Protokolle (beispielsweise Verschlüsselung wie TLS), mit denen man ihnen begegnen kann.

Network Slicing: Diese Technik ermöglicht das Bereitstellen von verschiedenen virtuellen Netzen auf einer gemeinsamen physischen Netzwerkinfrastruktur. Die einzelnen Slices erfüllen dann die unterschiedlichen Anforderungen verschiedener Anwendungsfälle. Die Eigenschaften von Slices lassen sich ohne Eingriff in die Hardware veränderten Anforderungen anpassen. Der wesentliche Vorteil des Slicing ist, dass beispielsweise Übertragungsraten, Latenzzeiten, Reichweiten, Verfügbarkeiten oder maximale Gerätedichte an die unterschiedlichen Anforderungen der Nutzer angepasst werden können. So stellen etwa Multimediaanwendungen andere Netzwerkanforderungen als Endgeräte des Internets der Dinge (IoT). Network Slicing kann auch dazu genutzt werden, system- oder unternehmenskritische Anwendungen vom übrigen Netz abzukoppeln und speziell abzusichern. Hier wird es die Aufgabe der Betreiber sein, die verschiedenen Slices gegeneinander zu isolieren.

Dezentralisierung: 5G erhöht die Funktionalität am Rand des Netzes und führt zu einer dezentraleren Architektur als in früheren Generationen von Mobilfunknetzen. Dies verbessert die Optionen für den Verbindungsaufbau und unterstützt das Mobile Edge Computing. Dieses Konzept ist eigentlich eine komplementäre Erweiterung von Cloud Computing. Verglichen mit dem herkömmlichen «zentralen» Cloudcomputing rückt die Intelligenz beim Edge Cloud Computing aber näher an die Nutzer heran. Dies erlaubt es, Daten ressourcenschonend an den Rändern des Netzes, beispielsweise in den Netzknoten, zu verarbeiten. Entsprechend eingesetzt, kann diese Dezentralisierung auch die Resilienz der Infrastruktur erhöhen.

4. Rechtliche Grundlagen in der Schweiz

Die in der Schweiz gültigen rechtlichen Grundlagen zur Sicherheit von Telekommunikationsnetzen sind durchwegs auch auf 5G anwendbar. Relevant sind:

- Das Fernmeldegesetz (FMG) – es regelt insbesondere die zuverlässige Versorgung der Schweiz mit Fernmeldediensten, die Grundversorgung, den störungsfreien Betrieb, die Persönlichkeitsrechte, den Wettbewerb.
- Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) – es regelt den Schutz der Persönlichkeit und der Grundrechte von Personen, deren Daten verarbeitet werden.
- Verordnung über Fernmeldedienste (FDV) – sie legt die Rahmenbedingungen fest, unter denen in der Schweiz Fernmeldedienste angeboten werden dürfen.
- Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022

5. Organisationen, die die 5G-Sicherheit voranbringen

International

Auf internationaler Ebene entwickeln mehrere Organisationen Empfehlungen, Standards und Instrumente für die 5G-Sicherheit. Die Arbeiten hierzu sind aber noch in Gang und auch der 5G-Standard als Ganzes wird noch weiterentwickelt. Zu wichtigen Organisationen gehören etwa:

- Die **EU**, unter anderem via ihre Agentur für Cybersicherheit **ENISA** (European Network and Information Security Agency)
- Das Europäische Institut für Telekommunikationsnormen **ETSI** (European Telecommunications Standards Institute) ist eine der drei grossen Normungsorganisationen in Europa und verfolgt das Ziel, weltweit anwendbare Standards für die Informations- und Kommunikationstechnik zu schaffen. asut vertritt die Schweizer Interessen im ETSI.
- Die Internationale Organisation für Normung (International Organization for Standardization, **ISO**) ist die internationale Vereinigung von Normungsorganisationen und gibt internationale Normen in allen Bereichen heraus mit Ausnahme der Elektrik und der Elektronik. Im Zusammenhang mit der Mobilfunkbranche sind vor allem ISO-Normen relevant, die Qualitätssicherung und Sicherheitsprozesse betreffen.
- Das 3rd Generation Partnership Project (**3GPP**) ist eine weltweite Kooperation von Standardisierungsgremien für die Standardisierung im Mobilfunk; konkret für UMTS, LTE und 5G/NR. Ihr Ziel ist es, technische Spezifikationen zu erstellen, die alle Aspekte der Mobilfunktechnik so präzise beschreiben, dass die Mobilgeräte aller Lieferanten in allen Mobilfunknetzen fehlerfrei funktionieren. Dazu gehört auch die Informationssicherheit.
- Die GSM Association (**GSMA**) ist die weltweite Industrievereinigung der GSM-Mobilfunkanbieter. Zusammen mit 3GPP hat sie das Network Equipment Security Assurance Scheme (NESAS) entwickelt. Diese Initiative bietet einen Rahmen für die Förderung der Sicherheit in der gesamten Mobilfunkbranche und steht allen Anbietern von Netzwerkausrüstung offen, die von 3GPP definierte Funktionen unterstützen.
- Das National Institute of Standards and Technology (**NIST**) ist eine Bundesbehörde der USA. Es ist für Standardisierungsprozesse, auch hinsichtlich der Sicherheit zuständig.
- Die Internationale Fernmeldeunion (englisch International Telecommunication Union, **ITU**) ist eine Sonderorganisation der Vereinten Nationen und die einzige völkerrechtlich verankerte Organisation, die sich weltweit mit technischen Aspekten der Telekommunikation beschäftigt. Sie ist Veranstalterin der Weltfunkkonferenz (World Radiocommunication Conference, WRC), die die Vollzugsordnung für den Funkdienst (Radio Regulations, RR) fortschreibt, sowie der Weltweiten Konferenz für internationale Fernmeldedienste (World Conference on International Telecommunications, WCIT), die die Vollzugsordnung für internationale Fernmeldedienste (International Telecommunication Regulations, ITR) fortschreibt.
- Die Transported Assets Protection Association (**TAPA**) gibt Standards zur Sicherheit von Betriebsstätten und Transporten heraus. Dies deckte einen Teil der Risiken in der Lieferkette ab.
- Der **Geneva Dialogue on Responsible Behavior in Cyberspace** ist ein Prozess zur Definition und Verbreitung global geteilter grundlegender Anforderungen an das sichere Design digitaler Produkte, an dem namhafte Hersteller beteiligt sind. Das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) nimmt hier eine führende Rolle ein und kofinanziert das Projekt.

National

Das Nationale Testinstitut für Cybersicherheit (**NTC**) in Zug wurde im November 2020 gegründet. Es soll ab 2022 als unabhängige Schweizer Organisation Cybersicherheits-Prüfungen für Einkäufer und Betreiber von kritischen Komponenten anbieten. Träger sind der Kanton Zug und das Nationale Zentrum für Cybersicherheit (NCSC).

6. Standards, Normen, Empfehlungen zur 5G-Sicherheit

Die oben erwähnten Organisationen geben die für die Branche relevanten Standards, Normen und Empfehlungen bezüglich Sicherheit heraus. Einige davon betreffen spezifisch 5G, andere sind allgemein in der IKT anwendbar und weitere gelten allgemein für die Industrie. Diese Werkzeuge ermöglichen den Schweizer Betreibern, eine eigene Strategie zu entwickeln und umzusetzen. Zu den Wichtigsten gehören:

		Wirkungsebene	
Instrument	**Beschreibung**	**Betreiber**	**Lieferant**
Norm ISO 27001 (Information security management)	Legt die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informations-Sicherheits-Managementsystems (ISMS) fest. Um Datenschutz und Informationssicherheit ganzheitlich gewährleisten zu können, werden auch individuelle IT-Risiken innerhalb der gesamten Organisation berücksichtigt. Alle Schweizer Betreiber pflegen ein ISMS. Die Norm ist umfassend, breit anerkannt, und zertifizierbar. Sie gilt generell für Datennetze und wird in der Schweiz von vielen Telekom-grosskunden angewendet. Mit der Richtlinie ISO 27001/2 liegt auch eine Beschreibung der Best-Practise für die Umsetzung vor.	x	x
EU-Toolbox 5G-Sicherheit	Ihr Kern ist ein risikobasierter Massnahmenkatalog zur 5G-Sicherheit. Die Toolbox deckt alle in der EU in 5G-Netzen eingesetzten Produkte (sowohl für reine 5G-Komponenten als auch für sonstige Komponenten der IKT) ab und gilt für alle Betreiber respektive deren 5G-Netze in der EU. Die Toolbox basiert auf einem praxistauglichen Ansatz und ist spezifisch auf Mobilfunknetze ausgerichtet. In der EU wird zurzeit eine Zertifizierung vorbereitet (Details siehe Kasten).	x	x
Norm ISO 22301 (Security and resilience - Business continuity management systems)	Zielt unabhängig von der Branche darauf ab, dass Organisationen ein Managementsystem haben, das ihnen erlaubt, bei Störungen ihre wichtigste Geschäftstätigkeit weiter betreiben können. Die Norm ist auf die gesamte IKT ausgerichtet und zertifizierbar.	x	

		Wirkungsebene	
Instrument	**Beschreibung**	**Betreiber**	**Lieferant**
Norm ISO 20243 (Open Trusted Technology Provider Standard (O-TTPS) - Mitigating maliciously tainted and counterfeit products)	Liefert eine Reihe von Richtlinien, Anforderungen und Empfehlungen, die spezifische Bedrohungen der Integrität von Hard- und Software während des gesamten Produktlebenszyklus betreffen. Insbesondere behandelt sie auch Bedrohungen im Zusammenhang mit böswillig manipulierten Produkten. Die Norm ist praxistauglich ausgelegt und zertifizierbar.		x
NESAS-Schema (Network Equipment Security Assurance Scheme)	Ein von 3GPP und GSMA definiertes Konzept, das die Sicherheit in der gesamten Mobilfunkbranche adressiert. Es definiert Anforderungen und einen Bewertungsrahmen für die sichere Produktentwicklung und einen sicheren Produktlebenszyklus. Insbesondere regelt es den Einsatz von Sicherheitstest von Netzkomponenten gemäss den Vorgaben der 3GPP. In der aktuellen Fassung basiert NESAS noch auf Selbstdeklaration, in der nächsten Version wird es zertifizierbar sein. Die grossen Netzwerkausrüster haben eine Bewertung ihrer Produktentwicklungs- und Lifecycle-Management-Prozesse mit NESAS erfolgreich abgeschlossen. Das NESAS-Schema ist spezifisch auf Mobilfunknetze ausgerichtet. Unternehmen können sich nach ihm auditieren lassen und die Audit Reports sind einsehbar auf www.gsma.com. Das NESAS-Schema wird auch eine Rolle bei der von der EU angestossenen Sicherheitszertifizierung für 5G spielen.		x
ETSI-Spezifikation TS 133.501 / 3GPP TS 33.501 (Security architecture and procedures for 5G System)	Spezifikation zur Sicherheitsarchitektur, also zu den Sicherheitsfunktionen und den Sicherheitsmechanismen für 5G-Netze. Abgedeckt werden auch die Sicherheitsverfahren, die innerhalb des 5G-Systems einschliesslich des 5G-Kernnetzes und des 5G-New-Radios durchgeführt werden. Die Spezifikation ist zertifizierbar und ihr zu folgen ist Pflicht, sowohl für Betreiber als auch für Lieferanten.	x	x
NIST-Standards	Diverse IKT-Sicherheitsstandards des US-amerikanischen National Institute of Standards and Technology (NIST). Sie sind auf die Rahmenbedingungen in den USA zugeschnitten und nicht generell auf die Schweiz übertragbar. Die Standards sind zertifizierbar und haben inhaltliche Überschneidungen mit ISO 27001.	x	x

		Wirkungsebene	
Instrument	**Beschreibung**	**Betreiber**	**Lieferant**
C-TPAT (Customs-Trade Partnership Against Terrorism)	Ein in öffentlich-privater Partnerschaft erarbeitetes Programm unter Leitung der Zoll- und Grenzschutzbehörde der USA für den erhöhten Schutz der Lieferkette privater Unternehmen zum Schutz vor Terroranschlägen. Dies erhöht auch den Schutz von IKT-Equipment vor Manipulationen während dem Transport. Nach C-TPAT kann zertifiziert werden. Auch wenn es sich dabei um ein US-amerikanisches Regelwerk handelt, bietet es praktische Ansätze zum Verbessern der Produktsicherheit.		x
TAPA-Standards (Transported Assets Protected Association)	Standards für Sicherheit in Betriebsstätten (Facility Security Requirements, FSR) und für den Transport (Trucking Security Requirements). TAPA ist ein weltweit akzeptierter Industriestandard und als solches zertifizierbar.		x
Norm ISO 28000 (Specification for security management systems for the supply chain)	Bietet eine umfassende Grundlage für das Sicherheitsmanagement in Lieferketten (Supply Chains). Insbesondere ermöglicht sie es, ein vollständiges System für die Sicherheit in der Lieferkette aufzubauen. Die Norm ist spezifisch auf die Sicherheit in der Logistik ausgerichtet und kann zertifiziert werden. Sie ergänzt insofern die ISO 27000, die sich mit Produktsicherheit befasst.		x

Exkurs: EU-Toolbox 5G-Sicherheit

Das EU-Instrument für die 5G-Sicherheit ist auf der Grundlage der EU-weit koordinierten Risikobewertung von 5G-Netzen entstanden. Es liefert eine Reihe von strategischen und technischen Sicherheitsmassnahmen, die es ermöglichen, Risiken wirksam zu mindern und den Aufbau sicherer 5G-Netze zu gewährleisten. Die 11 technischen Massnahmen (Technical Measures, TM) liefern einen Referenzrahmen für die Betreiber zur Umsetzung eigener Security-Massnahmen. Sie decken folgende Aspekte ab:

- TM01: Sicherstellen, dass die grundlegenden Sicherheitsanforderungen erfüllt werden (sicheres Netzwerkdesign und -architektur))
- TM02: Sicherstellen und Evaluieren der Implementierung von Sicherheitsmassnahmen in bestehenden 5G-Standards
- TM03: Sicherstellen einer strikten Zugriffskontrolle
- TM04: Erhöhen der Sicherheit von virtualisierten Netzwerkfunktionen
- TM05: Gewährleisten von sicherem 5G-Netzmanagement und -Betrieb sowie eines wirksamen Monitorings
- TM06: Stärken der physischen Sicherheit
- TM07: Stärken der Software-Integrität, sicheres Update- und Patch-Management

- TM08: Heben der Sicherheitsstandards in den Prozessen von Lieferanten durch robuste Beschaffungskonzepte
- TM09: Nutzen der EU-Zertifizierung für 5G-Netzkomponenten, Kundengeräte und/oder Prozesse von Lieferanten
- TM10: Nutzen der EU-Zertifizierung für andere, nicht 5G-spezifische IKT-Produkte und -Dienste (verbundene Geräte, Cloud-Dienste)
- TM11: Stärken von Resilienz- und Kontinuitätsplänen.

Für jede dieser Massnahmen liefert die Toolbox detaillierte Pläne zur Minderung aller festgestellten Risiken und Empfehlungen für die Umsetzung.

7. Massnahmen für die 5G-Sicherheit

Bei den Betreibern

Aus Sicht der Betreiber hat sich das bisherige Regime bei der Sicherheit im Mobilfunk bewährt. Deshalb soll es auch bei 5G beibehalten werden. Auf der einen Seite wird das Grundsätzliche durch den rechtlichen Rahmen geregelt, auf der anderen Seite sorgt die Branche in Eigenverantwortung – und notabene aus Eigeninteresse – für weitergehende Sicherheit. Dazu gehört insbesondere, dass die Betreiber die Kontrolle über die Kundendaten und den Kommunikationsverkehr haben und Lieferanten oder Dienstleister nur mit dem Einverständnis der Betreiber und kontrolliert durch diese darauf zugreifen können. Zudem stützt sich die Branche auf technik- und herstellerneutrale internationale Standards, Normen und Empfehlungen. Dies hat auch den Vorteil, dass neue Entwicklungen, Risiken und Anforderungen viel rascher umgesetzt werden können, als dies im Gesetzgebungsprozess möglich wäre.

Betreffend Informationssicherheit empfiehlt sich die Norm ISO 27001 (Information-Security-Management-System) als Basisinstrument. Zu ihr liegen auch detaillierte Ausführungsvorschriften vor (ISO27001/2). Dieser ISO-Standard hat folgende Vorteile:

- Er ist universell, international anerkannt und wird von einem neutralen Gremium herausgegeben.
- Er wird verbreitet angewendet und hat sich auch in anderen Branchen bewährt. So referenziert etwa der Verband Schweizerischer Elektrizitätsunternehmen VSE in seinem Handbuch zur Umsetzung von OT-Sicherheit in kritischen Infrastrukturen der Schweiz [1] auf diesen Standard.
- Er kann zertifiziert werden.
- Er berücksichtigt auch die individuelle IT-Risiken innerhalb einer Organisation und hilft, Datenschutz und Informationssicherheit ganzheitlich zu gewährleisten
- Er wird von den Schweizer Telekomanbietern bereits angewendet.
- Er ist auch von der Telekom-Kundschaft anerkannt und wird von ihr genutzt. Bei Grosskunden ist ein Zertifikat nach ISO 27001 mittlerweile die Grundvoraussetzung, damit sie überhaupt mit einem Telekomanbieter zusammenarbeiten.
- Es ist eine klare Tendenz festzustellen, dass die ISO 27001 sich international zum Massstab für die Informationssicherheit entwickelt.

Als ergänzendes, 5G-spezifisches Instrument bieten sich die technischen Massnahmen der EU-Toolbox 5G-Sicherheit an. Sie liefert einen umfassenden Ansatz zu Minderung von spezifischen Risiken und wird in näherer Zukunft auch zertifiziert werden können.

[1] https://www.ee-news.ch/de/article/41092/vse-handbuch-zur-umsetzung-von-ot-sicherheit-in-kritischen-infrastrukturen-der-schweiz&page=1

In der Lieferkette

Geht es um die Resilienz der kritischen Infrastruktur «Mobilfunknetze» zeigen sich die Vorteile des Infrastrukturwettbewerbs in der Schweiz, wie er im FMG vorgesehen ist. Heute bieten drei Betreiber ihre Dienste über eigene und unabhängige Netze an. Sie arbeiten zudem mit drei unterschiedlichen Systemlieferanten zusammen. Damit kann davon ausgegangen werden, dass beispielsweise vom kurzfristigen Ausfall eines Lieferanten nur ein Teil der Netze betroffen ist. Damit ist die Schweizer Mobilfunkinfrastruktur in sich bereits recht resilient.

Weiter zur Sicherheit der Mobilfunknetze trägt bei, dass die Lieferanten ihrerseits ständig daran arbeiten, die Qualität ihrer eigenen Lieferkette zu sichern. Als Basis hierfür dient ihnen die Norm ISO 28000. Die relevanten Transport- und Logistikunternehmen sowie Lieferanten von wichtigen Netzkomponenten sind nach ihr zertifiziert, was bereits für eine Grundsicherheit sorgt. Zur Behandlung von spezifischen Risiken werden beispielsweise folgende weiter Standards herbeigezogen:

- ISO 20243 (Produktintegrität)
- TAPA-Standards FSR (Facility Security Requirements,) und TSR (Trucking Security Requirements).
- C-TPAT (Schutz vor terroristischen Aktionen im Rahmen der Lieferkette)

Aus Sicht der Branche steht damit auch für die Sicherheit in der Lieferkette ein bewährtes Instrumentarium zur Verfügung. Die Betreiber fordern von den Lieferanten die entsprechenden Zertifikate und Nachweise ein.

Was die Bedrohung durch Fremdstaaten und spezialisierte Organisationen angeht: Sie kann durch das Anwenden der einschlägigen Normen und Standards zwar vermindert, aber nicht ausgeschlossen werden. Wenn ein Staat Netzkomponenten kompromittieren will, dann wird er einen Weg dazu finden. Je nach Herkunft kann das schon in der Hardware- oder Softwareentwicklung sein oder erst später beim Transport respektive bei Software-Updates.

Vielversprechend bezüglich der Produktsicherheit ist die Gründung des Nationalen Testinstituts für Cybersicherheit (NTC) durch den Kanton Zug mit Unterstützung des Nationalen Zentrums für Cybersicherheit (NCSC). Dort sollen ab 2022 kritische Komponenten hinsichtlich Schwachstellen geprüft werden.

Ein interessanter, wenn auch eher langfristig ausgelegter Ansatz ist die Initiative «**Geneva Dialogue on Responsible Behavior in Cyberspace**». Sie hat sich zum Ziel gesetzt, ähnlich wie die Menschenrechtskonvention eine internationale Übereinkunft zur Sicherheit in der IKT zu etablieren. Damit zielt sie vor allem auf Staaten, die die Cybersicherheit durch Manipulationen an Geräten und Komponenten gefährden.

8. Offene Punkte auf Nutzerseite

Neben den Risiken aus dem Betrieb und aus den Lieferketten spielen bei 5G vor allem auch nutzerbezogene Aspekte eine Rolle. Hier gilt es insbesondere die Konfiguration und den Betrieb von IoT-Geräten abzusichern – dies vor allem wegen der stark steigenden Anzahl von verbundenen Geräten. Zwar ist momentan 5G noch nicht die wichtigste Zugangstechnik für IoT, aber das wird sich in Zukunft ändern.

Prinzipiell bietet 5G die Möglichkeit, den Datenverkehr von IoT-Geräten in separaten Network-Slices abzuwickeln. Dadurch liessen sich andere Anwendungen auf dem Netz vor Einflüssen durch IoT schützen. Das ändert aber nichts daran, dass viele Endgeräte ab Werk nicht auf Sicherheit ausgelegt und vorkonfiguriert werden (Stichwort Security by Design). In diesem Zusammenhang wären etwa zu nennen:

- Heute haben viele Geräte ab Werk unsichere Standard-Passwörter und führen die Nutzer ungenügend bezüglich des Setzens von eigenen, sicheren Passwörtern.
- Oft stehen nicht benötigte Schnittstellen und Ports offen, ohne dass die Nutzer darauf hingewiesen werden.
- Die Firmware der Geräte wird nicht, zu spät oder nicht über die ganze Nutzungsdauer mit Sicherheits-Updates versorgt

Solche Risiken entziehen sich dem Einfluss der Netzbetreiber weitgehend, weil die meisten IoT-Endgeräte weder von ihnen geliefert noch von ihnen geprüft werden. In der Regel werden sie von den Nutzern auf dem freien Markt beschafft. Die dadurch entstehenden Risiken sind aber massiv, weil jedes unsicher konfigurierte Endgerät ein Angriffsvektor ist und ihre Anzahl stark steigen wird.

Wie mächtig kompromittierte Endgeräte als Angriffswaffe sein können, zeigt ein Vorfall beim Internetdienstleister Dyn von 2016. Dabei wurden Hunderttausende kompromittierter Endgeräte zu einem Botnetz zusammengefügt und für eine DDoS-Attacke orchestriert. Als Folge waren die betroffenen Online-Dienste (unter anderem Twitter, Pinterest, Reddit) zeitweise gestört. Ursache war der ungenügende Schutz von Endgeräten wie Router und Überwachungskameras.

9. Fazit und Standpunkt der asut

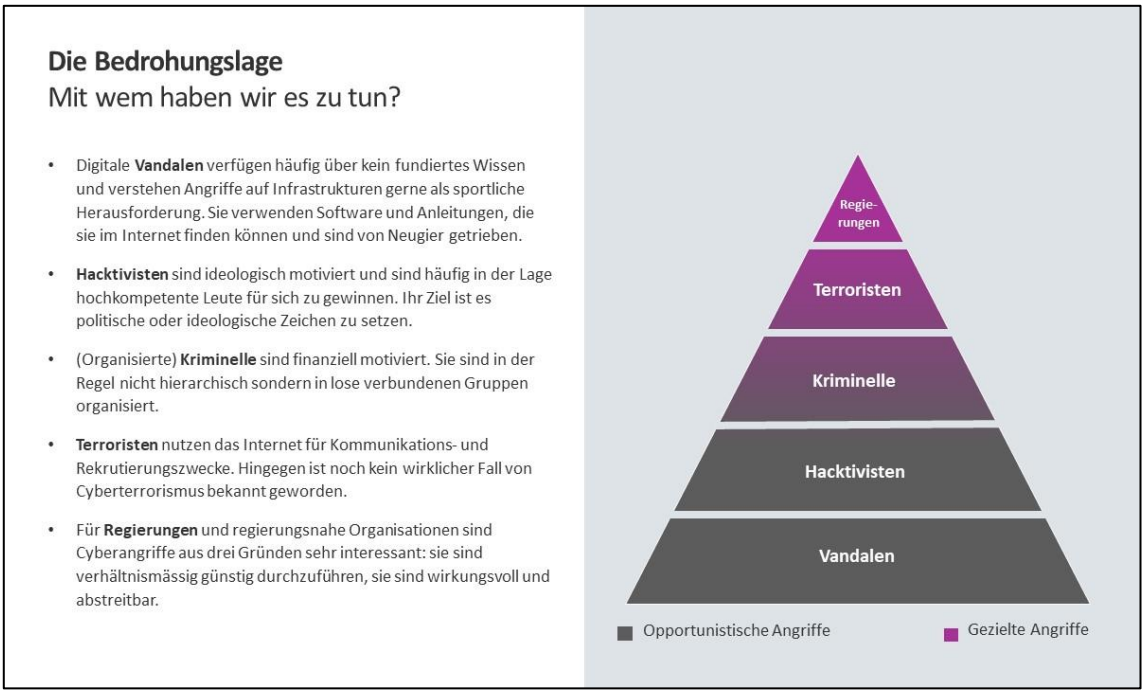
- Bereits bei der Konzeption von 5G wurde der Cybersicherheit ein hoher Stellenwert beigemessen. 5G ist daher deutlich sicherer als alle bisherigen Mobilfunktechnologien einschliesslich 4G.
- Cybersicherheit liegt im ureigenen Interesse der Telekommunikationsunternehmen. Insbesondere Firmenkunden aus sensiblen Bereichen fordern hier ein rigoroses Engagement und auch die relevanten Nachweise. Davon profitieren auch die Privatanwender.
- Die bereits bei 3G/4G-Netzen angewendeten Konzepte hinsichtlich Cybersicherheit haben sich bewährt und sollen auch für 5G angewendet werden.
- Die Risiken von 5G-Netzen sollen weiterhin technik- und herstellerneutral beurteilt werden.
- Die erforderlichen Instrumente sind in Form von internationalen Normen, Standards und Empfehlungen vorhanden und werden sowohl von den Betreibern als auch von den Lieferanten angewendet.
- Als Basisinstrument für die Betreiber empfiehlt sich die Norm ISO 27001. Sie behandelt die Cybersicherheit universell und wird breit eingesetzt – nicht nur in der IKT-Branche.
- Als Basisinstrument für die Sicherheit in der Lieferkette eignet sich die Norm ISO 28000. Alle relevanten Transport- und Logistikunternehmen sowie die Lieferanten von wichtigen Netzkomponenten sind nach ihr zertifiziert. Für Aspekte, die die ISO 28000 nicht (genügend) abdeckt, soll sie durch spezifischere Instrumente wie ISO 20243, die TAPA-Standards oder allenfalls C-TPAT ergänzt werden.
- Manipulationen von Fremdstaaten oder spezialisierten Organisationen an Netzkomponenten lassen sich mit diesem Instrumentarium und technischen Vorkehrungen nicht abschliessend verhindern. Ob hier weitergehende vorsorgliche Massnahmen ergriffen werden sollen, muss politisch abgewogen und entschieden werden. Einen interessanten Ansatz verfolgt der Kanton Zug mit dem Nationalen Testinstitut für Cybersicherheit, das ab 2022 kritische Komponenten auf Sicherheitslücken untersuchen will. Förderungswürdig in diesem Zusammenhang erscheinen internationale Initiativen wie der Geneva Dialogue on Responsible Behavior in Cyberspace.

10. Anhang

Bedrohungspyramide

Bei den Angreifern lässt sich unterscheiden zwischen solchen, die opportunistisch und solchen, die gezielt vorgehen. Bei mehrheitlich opportunistischen Akteuren wie Vandalen (z. B. Script Kiddies) oder Hacktivisten kann davon ausgegangen werden, dass sie vor allem Schwachstellen ausnützen, um sich zu bereichern oder zu profilieren. Ihnen lässt sich entgegengetreten, indem man Schwachstellen so weit beseitigt oder abschwächt, dass sich ein Angriff nicht lohnt.

Anders verhält es sich bei Akteuren, die gezielt vorgehen. Diese Organisationen – vorab Staaten und Terroristen - wollen ein bestimmtes Ziel erreichen und werden dies konsequent und mit dem Einsatz von grossen personellen und finanziellen Mitteln verfolgen. Gegen solche Akteure vorzugehen, gestaltet sich massiv schwieriger und kostenintensiver.



Die Bedrohungspyramide in der Cybersicherheit (Quelle: Swisscom)

Angriffsmethoden und Ziele (Auswahl)

Advanced Persistent Threats (APT) sind technisch fortschrittlich, schwierig aufzuspüren und zu beseitigen. Ihr Ziel ist es, dauerhaft unerkannt Spionage zu betreiben oder Systeme im Bedarfsfall fernsteuern zu können. Hierzu werden oft verschiedene Angriffstechniken kombiniert. Ziel von APT ist es, meist tief in Systemen steckende Software und Hardware so zu manipulieren, dass sie bei Bedarf kontrolliert werden kann. Anfällig sind etwa Schnittstellen, Firmware oder elektronische Komponenten. Solche Angriffe vorzubereiten benötigt sehr viel Know-how, Ressourcen und Zeit. Deshalb werden sie meistens im Auftrag von Regierungen, Geheimdiensten oder grossen Konzernen in Auftrag gegeben.

Botnetze dienen dazu, sich über infizierte Geräte Zugriff auf Daten und Ressourcen im Netz zu verschaffen oder die Geräte fernzusteuern. Der Begriff stammt aus dem Englischen: bot (kurz für robot) und net (Netz). Ein bösartiger Bot ist ein durch Malware infiltriertes und gekapertes Gerät. Davon betroffen kann eine breite Palette von verbundenen Geräten sein. Sobald mehrere solcher Bots zusammengeschlossen sind, spricht man von einem Botnetz. Die

Cyberkriminellen, die die Malware über das Internet streuen und die infiltrierten Geräte kontrollieren, werden als Botmaster oder Botnet-Operator bezeichnet.

DDoS-Attacken (Distributed Denial of Service) zielen auf die Überlastung von Servern, Online-Services oder ganzer Netzwerke. Sie können immense Schlagkraft erreichen, weil ein Angreifer dabei eine Vielzahl gekaperter Rechner, Server oder kompromittierter IoT-Endgeräte nutzt. Ferngesteuert über einen Command & Control-Rechner greifen diese Geräte im Verbund als Botnetz ein Ziel an. DDoS-Attacken werden über alle Branchen hinweg eingesetzt, um beispielsweise Schutzgeld einzufordern. Auch in der Cyberspionage zählen DDoS-Angriffe zum Standardrepertoire.

Identitätsdiebstahl, auch Identitätsmissbrauch oder Identitätsbetrug genannt, dient Angreifern dazu, die Personendaten von anderen für Angriffe zu nutzen. Um an die nötigen Informationen zu kommen werden Techniken wie Spoofing, Phishing, Pharming oder Vishing eingesetzt.

Malware ist ein Sammelbegriff für Software, die Schaden anrichten soll. Er stammt aus dem Englischen und bedeutet «Malicious (bösartige) Software». Im Deutschen werden die Begriffe Schadprogramm oder Schadsoftware verwendet. Zur Malware gehören etwa Viren, Würmer oder Trojaner. Die Auswirkungen von Malware reichen von harmlosen Störungen über Erpressungsversuche bis hin zu gross angelegten Attacken, die ganze Systeme infiltrieren, lahmlegen oder autonom steuern. Malware bildet die Basis für die meisten anderen Angriffsmethoden.

Ein **Man-in-the-Middle-Angriff** (MITM-Angriff) ist ein Konzept, um Datenströme abzugreifen oder sogar zu manipulieren. Dabei stellt sich der Angreifer physisch oder logisch zwischen zwei Kommunikationspartner, und täuscht vor, jeweils der andere zu sein. So bleibt er unentdeckt und erhält die Kontrolle über den Datenverkehr zwischen den Netzwerkteilnehmern. Solche Angriffe richten sich häufig auf Prozesse, die mit finanziellen Transaktionen verbunden sind.

Unter **Peer-to-Peer-Spionage** versteht man das Ausspionieren von privaten Unternehmen durch andere private oder sonderprivatrechtliche, parastaatliche Unternehmen. Davon unterschieden werden muss die **Wirtschafts- und/oder die Wehrspionage** durch nichtstaatliche, parastaatliche oder staatliche Organe, welche sich gegen andere Staaten oder gegen private Unternehmen richten kann.

Physische Gewalt; neben den logischen Angriffsmethoden gibt es selbstverständlich auch physische. Hierzu gehören etwa terroristische Angriffe oder Sabotage direkt auf der Hardware-Ebene.

Ransomware ist ein Kofferwort aus den Begriffen Ransom (Lösegeld) und Software. Ransomware gehört zu den Schadprogrammen (Malware), mit deren Hilfe sich Kriminelle Zugang zu Daten oder ganzen Netzwerken verschaffen. Ihr Ziel ist es meist, den Zugriff auf die Daten zu blockieren, um Lösegeld zu erpressen. Hierzu werden die Daten entweder verschlüsselt oder in einen passwortgeschützten Bereich verschoben.