Sustainable Cyber Resilience im IKT-Sektor:

Informationstechnik und Telekommunikation

Whitepaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

09/2018

Management Summary

Informationstechnik und Telekommunikation zählen zu den kritischen Infrastrukturen und sind ein attraktives Ziel für Hacker. Um für angemessenen Schutz zu sorgen, reicht es nicht mehr aus, reaktive Maßnahmen zu ergreifen. Stattdessen müssen Unternehmen einen Zustand der Sustainable Cyber Resilience anstreben: der nachhaltigen Widerstandsfähigkeit. Dabei handelt es sich um ein umfassendes Konzept, das eher strategisch als technologisch ausgerichtet ist und einen Schritt weiter geht als IT Security. Sustainable Cyber Resilience sorgt zum einen dafür, Angriffsflächen zu verringern. Zum anderen stellt sie sicher, dass Unternehmen ihren Betrieb auch im Falle eines Angriffs aufrechterhalten und ihre angestrebten Geschäftsziele erreichen können – unter Berücksichtigung der Wirtschaftlichkeit. Dieses Whitepaper zeigt, warum Sustainable Cyber Resilience für den Sektor Informationstechnik und Telekommunikation so wichtig ist, was sie bedeutet und wie sie sich mithilfe von Vulnerability Management umsetzen lässt.

Inhalte

Einleitung

Sustainable Cyber Resilience ist für Unternehmen aller Branchen wichtig. Unverzichtbar ist sie aber im Bereich der kritischen Infrastrukturen (KRITIS). Darunter fallen laut Definition der Bundesregierung „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." KRITIS-Organisationen müssen sich daher besonders gut gegen Cyber-Angriffe schützen – das schreibt der Gesetzgeber vor. Die EU begann bereits 2006 mit dem European Programme for Critical Infrastructure Protection (EPCIP) und erweiterte und ergänzte dieses in den folgenden Jahren. Mitgliedsstaaten setzen die EU-NIS Direktive in nationales Recht um, Deutschland beispielsweise mit dem IT-Sicherheitsgesetz (IT-SIG). Große Wirtschaftsnationen haben bereits Regulierungsinstanzen entwickelt. In den USA ist dies zum Beispiel das US National Institute of Standards and Technology und in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI).

In Deutschland sind die kritischen Infrastrukturen in 9 Sektoren eingeteilt. Einer davon ist Informationstechnik und Telekommunikation (IKT). Er umfasst Unternehmen, die die technische Infrastruktur für die Sprach- und Datenkommunikation bereitstellen sowie solche, die Datenverarbeitungseinrichtungen für Dritte und IT-Hosting betreiben. Sowohl im Privatleben als auch im Beruf spielen moderne Informations- und Kommunikationstechnologien heute eine wichtige Rolle. So würde ohne Internet und Telefon die Arbeit in den meisten Unternehmen nahezu zum Erliegen kommen. Nicht nur sind Mitarbeiter auf die Kommunikationstechnik angewiesen, auch zentrale Computersysteme müssen heute miteinander Daten austauschen. Zudem bildet eine funktionierende Kommunikationsinfrastruktur die Basis für das Internet der Dinge und Industrie 4.0. Aufgrund dieser hohen Abhängigkeiten hat es weitreichende Folgen, wenn Telefon- und Datennetze ausfallen. Auch andere kritische Infrastrukturen wie die Trinkwasserversorgung oder der Betrieb in Krankenhäusern könnten beeinträchtigt werden. Notrufe würde nicht mehr funktionieren und die Regierung könnte ihre Bürger nicht mehr zeitnah über Gefahrensituationen informieren. Darüber hinaus sind Cyber-Angriffe auf die Kommunikationsinfrastruktur auch attraktiv für Terroristen und Geheimdienste, um sensible Daten mitzulesen und auszuspionieren.

Beispiele für Cyber-Attacken auf Infrastrukturen der Informationstechnik und Telekommunikation

In den vergangenen Jahren gab es weltweit bereits zahlreiche Angriffe auf kritische Infrastrukturen im IKT-Sektor. So wurde der halbstaatliche belgische Telekommunikationsanbieter Belgacom zwischen 2010 und 2013 Opfer einer groß angelegten Späh-Attacke. Laut Unterlagen des Whistleblowers Edward Snowden steckte der britische Geheimdienst GCHQ hinter dem Hack – so berichtete das Nachrichtenmagazin „Der Spiegel". Demzufolge hatte der GCHQ eine ausgefeilte Malware in Computer von Belgacom-Mitarbeitern eingeschleust und sich von dort aus zu zentralen Routern vorgearbeitet. So konnte der Geheimdienst über mehrere Jahre hinweg den Datenverkehr auslesen, der über die Belgacom-Netze geleitet wurde. Zu den Kunden des Telekommunikationsanbieters zählen unter anderem die Europäische Kommission, das Europäische Parlament und der Europäische Rat. Sicherheitsexperten hatten den Hack im Sommer 2013 entdeckt.

Im Oktober 2016 sorgte ein Cyber-Angriff auf den US-Netzwerkdienstleister Dyn für Aufsehen. Er bietet den Service DynDNS, eine grundlegende Funktion für das Internet. DynDNS verknüpft Domain-Namen mit Netzwerkadressen und sorgt so dafür, dass die richtige Webseite angezeigt wird, wenn ein Anwender eine www-Adresse in den Browser eingibt. Mit einer Denial of Service-Attacke überlasteten Hacker den Dienst und legten ihn lahm. Dadurch waren große Internetdienste-Anbieter wie Twitter, Paypal, Netflix und Amazon zeitweilig in Teilen der USA und Europas nicht erreichbar. Für ihre Attacke nutzten die Cyber-Kriminellen ein IoT-Botnetz, das sie mit der Schadsoftware Mirai aufgebaut hatten.

Ein Mirai-ähnliches Botnetz kam auch beim Angriff auf Router der Deutschen Telekom zum Einsatz, der im November 2016 bei mehr als 900.000 Kunden das Internet und die Internettelefonie lahmlegte. Ein Hacker hatte eine Sicherheitslücke in Routern des Herstellers Zyxel ausgenutzt, sie mit der Malware infiziert und in ein Botnetz eingebunden. Zwar handelte es sich bei den Telekom-Routern um Geräte eines anderen Herstellers, sodass die Versuche, sie zu infizieren, fehlschlugen. Die andauernden Attacken brachten die Router jedoch zum Absturz. Im Februar 2017 wurde der Hacker, der sich selbst „Spiderman" nannte, gefasst. Nach eigenen Angaben hatte er den Angriff nicht speziell auf die Telekom abgezielt, sondern wollte Router welt-

weit infizieren. Den Auftrag dafür habe er von einem Telekommunikationsunternehmen aus Liberia bekommen, das mit dem Botnetz die Konkurrenz im eigenen Land aushebeln wollte.

IT-Systeme und Prozesse im IKT-Sektor

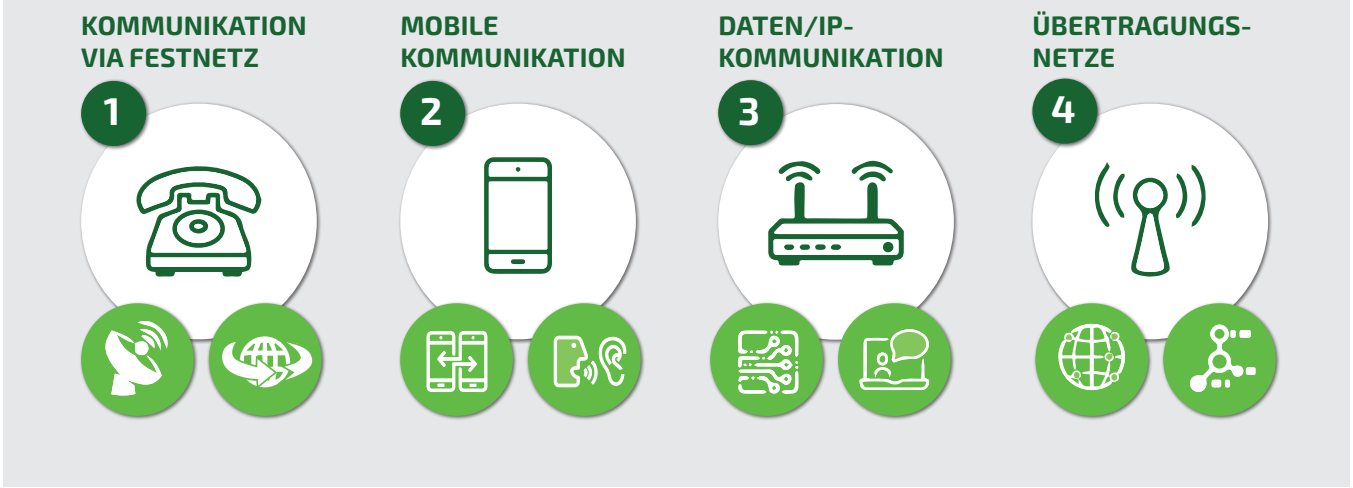
Kommunikation ist ein unverzichtbarer Enabler für andere Geschäftsprozesse, wie die Grafik unten verdeutlicht. Festnetzkommunikation (1) ist für das globale Transport- und Finanzwesen eine Grundfunktionalität für die Koordination und Verifikation von Geschäften. Die Mobilkommunikation (2) ist gerade mit den sogenannten Over-the-Top-Applikationen auf Verschlüsselung und Quality-of-Service der Sprache an sich angewiesen. Ähnliches gilt für die reine IP-basierte Kommunikation (3) von privaten Haushalten und Unternehmen, bereitgestellt zum Beispiel über DSL- oder Kabel-Anschluss. Die entsprechenden Zugangsserver der Provider sind für Angreifer interessante Ziele. Ziele sind auch die Übertragungsnetze (4), da sie sowohl global als auch national das verbindende Element für viele andere kritische Infrastrukturen sind.

Für die Bereitstellung, den Betrieb und die Verwaltung von Telekommunikations-Infrastrukturen kommen eine Vielzahl verschiedener IT-Systeme zum Einsatz. Sie umfassen Technologien für die unterschiedlichen Netztypen wie Mobilfunknetz, Festnetz, Breitbandkabel, Glasfaserkabel oder Satellitennetz. Gängige Systeme sind zum Beispiel Basisstationen und Funkmasten, Leitungen und Netzanschlüsse, Netzwerkmanagementzentren, Vermittlungssysteme, Überwachungs- und Steuerzentralen und Backbone-Komponenten wie Router und Switches. Nicht zu vergessen sind die Systeme auf Kundenseite wie Kabelmodems und Router. Kunden und Unternehmen kommunizieren über digitale Schnittstellen wie Portale in der Cloud oder mobile Apps miteinander. Dazu kommen Systeme zur Unternehmensadministration und zur Kundendatenverwaltung. Sie enthalten sensible Geschäftsgeheimnisse oder personenbezogene Daten, die unter die Europäische Datenschutz-Grundverordnung (DSGVO) fallen. Um einen Zustand der Sustainable Cyber Resilience zu erreichen, müssen Unternehmen aus dem IKT-Sektor das gesamte Spektrum der vernetzten Systeme, Geräte und Applikationen berücksichtigen.

Besondere Herausforderungen für Resilience im IKT-Sektor

Die Digitalisierung hat den IKT-Markt stark verändert. Immer mehr Dienste verlagern sich heute auf IP-Netze. So hat die klassische Festnetz-Telefonie ausgedient und wird zunehmend durch die Internettelefonie (VoIP) ersetzt. Die Deutsche Telekom hatte bereits 2016 angekündigt, all ihre Festnetzanschlüsse bis Ende 2018 auf IP umzustellen. Bei 90 Prozent ihrer Kunden ist dies bereits geschehen. Auch das Fernsehen und Videostreaming wird heute in vielen Haushalten über das IP-Netz übertragen. Es kommt also zu einer zuneh-

IKT als Enabler anderer Prozesse



menden Vereinheitlichung von Kommunikationsnetzen und Serversystemen. Das macht sie gleichzeitig auch attraktiv für Angreifer, denn Hacker können mit einer Attacke auf das IP-Netz viele Dienste auf einen Schlag kompromittieren und massiven Schaden anrichten.

Außerdem hat die mobile Kommunikation und Datennutzung stark zugenommen. Kunden surfen heute mit dem Smartphone im Internet, streamen Videos und laden Fotos in Social-Media-Kanäle hoch. Das erfordert immer leistungsfähigere Mobilfunknetze. Sehnlichst erwartet wird der neue Mobilfunkstandard 5G, der Kommunikation nahezu in Echtzeit ermöglichen soll – eine wichtige Voraussetzung beispielsweise für zeitkritische IoT-Anwendungen. Dies bringt jedoch auch zunehmende technische Komplexität und neue Anforderungen an die IT-Sicherheit mit sich. Gleichzeitig wächst mit dem Grad der Vernetzung die Angriffsfläche.

Auch auf organisatorischer Seite gibt es Herausforderungen für die Etablierung von Sustainable Cyber Resilience. Denn an Telekommunikations-Infrastrukturen sind häufig viele verschiedene Unternehmen und Subunternehmen beteiligt, die sich teilweise auch in anderen Ländern befinden. Dadurch gibt es verschachtelte Verantwortlichkeiten, die ein einheitliches, durchgängiges Schutzniveau erschweren.

Vulnerability Management als wichtiger Baustein für Sustainable Cyber Resilience

Resilienz ist ein kontinuierlicher Prozess. Er verstärkt die Fähigkeiten eines Unternehmens, einer Attacke zu widerstehen, und versetzt es in die Lage, auch während eines Angriffes zu funktionieren. Um dies zu erreichen, ist es wichtig, die Angriffsfläche zu reduzieren und so die Basis zu stabilisieren. Das bedeutet, Schwachstellen zu identifizieren, die von einem Angreifer ausgenutzt werden könnten. Letztlich heißt es, dem Angreifer einen Schritt voraus zu sein.

Greenbones Schwachstellenmanagement funktioniert mit dem Greenbone Security Manager (GSM) und ist dafür gedacht, Resilience durch einen kontinuierlichen Prozess nachhaltig zu etablieren. Dieser besteht aus den folgenden, größtenteils automatisierten Schritten:

Widerstandsfähigkeit durch den Schwachstellen-Management-Prozess

Prepare

Im ersten Schritt geht es darum, den Kontext zu IT-Sicherheits-Policies, Risikobewertungen, Unternehmensprozessen und unternehmenskritischen Systemen herzustellen. Was will ich wie und wie intensiv schützen? Wie viel Risiko bin ich bereit zuzulassen? In Konfigurationsrichtlinien legen die IT-Verantwortlichen fest, was im Rahmen der Sicherheitsvorgaben erlaubt ist. Diese Richtlinien können dann mit einer technischen Kontrolle im GSM verknüpft werden. Hinzu kommen Informationen rund um den Security Workflow und die Verantwortlichkeiten. Wer muss informiert sein? Wer entscheidet, ob eine Schwachstelle behoben werden soll oder darf? Wer behebt sie?

Identify

Jetzt folgt die Analyse der Ist-Situation. Ein Vulnerability Scan stellt fest, welche Schwachstellen die Infrastruktur aktuell aufweist und wo sie von Konfigurationsvorgaben abweicht. Dabei muss sichergestellt werden, dass die Datenbank mit den Schwachstelleninformationen auf dem neuesten Stand ist. Außerdem wird identifiziert, wo genau sich die Schwachstelle oder Abweichung von der Norm befindet, und hinterfragt, wie belastbar die gefundenen Ergebnisse sind. Das dient dazu, False Positives und False Negatives zu vermeiden. Greenbone hat dafür das Feature QoD „Quality of Detection“ eingebaut. Es nennt einen Prozentwert, mit welcher Wahrscheinlichkeit die Schwachstelle tatsächlich existiert.

Classify

Die gesammelten Informationen werden jetzt nach unterschiedlichen Kriterien eingeteilt, die das Unternehmen individuell festlegen kann – zum Beispiel wo ein System physikalisch steht, zu welcher Abteilung es gehört, in welchem Netzsegment es sich befindet und welche Funktion es im Unternehmen erfüllt. Diese Einteilung ist unabhängig von der Kritikalität der Schwachstelle. Classify macht nichts anderes, als die Funde anhand der vorhandenen Merkmale zu gruppieren. Wichtig hierbei ist, dass eine solche Gruppierung im Sinne der Automatisierung in Regeln abgebildet werden kann.

Prioritize

Jetzt wird priorisiert, was auf Basis der Ziele aus dem ersten Schritt „Prepare“ mit den gefundenen Schwachstellen aus dem Schritt „Identify“ anhand der Einteilungen von „Classify“ am wichtigsten und damit als Erstes zu tun ist. Welcher Fund hat die größte Auswirkung und muss zuerst bearbeitet werden?

Assign, Mitigate & Remediate

Die technischen Erkenntnisse müssen in einem Arbeitsprozess münden, der zur Schließung der Schwachstelle führt. Ein Vulnerability-Management-Prozess sollte regeln, wer wann welche Informationen zu entdeckten Schwachstellen bekommt, wer für welche Schritte verantwortlich ist und welche Mittel und Wege zur Verfügung stehen. Das Vulnerability-Management-System sollte hier so viele Informationen wie nur möglich mitliefern. Die Handlung kann auch über den Austausch mit anderen Workflow Tools initiiert werden, zum Beispiel einem ISMS, einem Ticket-System für Helpdesks oder einem SIEM-System zur weiteren Korrelation von Security Events beziehungsweise Incidents.

Store & Repeat, Improve

Die letzten Schritte dienen der Auditierbarkeit des Systems nach ISO 27000 sowie der Verbesserung, Veränderung und Anpassung. Store & Repeat protokolliert wichtige Informationen, zum Beispiel, wann eine Schwachstelle zum ersten Mal gefunden wurde, wann sie gemeldet wurde und wie lange es gedauert hat, sie zu beheben. Dies hilft bei der Analyse von Sicherheitsvorfällen. „Improve“ ist der Übergang zu einem erneuten Durchlauf des Vulnerability-Management-Prozesses, der wieder mit „Prepare“ beginnt. Jetzt können Sicherheitsverantwortliche die Zielsetzung verfeinern, verschärften oder an veränderte Policies anpassen. Schwachstellenmanagement ist kein statisches System, sondern ein dynamischer Prozess, bleibt aber immer automatisierbar.

Grenzen von Vulnerability Management

Vulnerability Management ist ein wichtiger Baustein, um Sustainable Cyber Resilience zu erreichen. Es ist jedoch nur ein Element in einer umfassenden Gesamtarchitektur. Für nachhaltige Cyber Security und Widerstandsfähigkeit sind noch viele weitere Faktoren zu berücksichtigen, die ineinandergreifen müssen. Neben der Absicherung der Systeme gegen Hackerangriffe dürfen Unternehmen auch die physische Sicherheit nicht vernachlässigen. Zudem spielen organisatorische Maßnahmen eine wichtige Rolle. Unternehmen müssen genau festlegen und dokumentieren, wie Security-Prozesse aussehen und wer welche Aufgaben und Verantwortung übernimmt. Außerdem dürfen Unternehmen den Faktor Mensch nicht vergessen. Eine wichtige Präventionsmaßnahme sind nach wie vor Schulungen zur Sensibilisierung für IT-Risiken. Denn viele Mitarbeiter sind sich nicht bewusst, wie gefährlich Fehlverhalten oder Unachtsamkeit sein kann.

Nicht umsonst schreiben zahlreiche Richtlinien und Gesetze Schwachstellen-Scans und Risikobewertung vor. So erwartet zum Beispiel die EU-DSGVO ein implementiertes Schwachstellenmanagement. Auch für eine ISO 27001-Zertifzierung ist dies Voraussetzung. Die Fähigkeit, Schwachstellen zeitnah aufzufinden, zu priorisieren und zu beseitigen, ermöglicht es Unternehmen, ihre IT-Systeme kontinuierlich sicherer zu machen und die Angriffsfläche zu reduzieren. Das ist ein laufender Prozess, der nie abgeschlossen sein darf. Für Organisationen, die unter die KRITIS fallen, ist Vulnerability Management Pflicht.

Über Greenbone

Greenbone Networks wurde 2008 von Netzwerksicherheits- und Open-Source-Experten gegründet. Hauptsitz des international agierenden Privatunternehmens ist Osnabrück. Die Greenbone Security Manager (GSM) basieren auf Open Source Software. Sie analysieren IT-Netzwerke auf Schwachstellen und liefern Sicherheitsberichte sowie Hinweise zur Behebung, bevor Angreifer die Sicherheitslücken ausnutzen können. Bestandteil der Lösungen ist ein tägliches, automatisches Security Update. Es bündelt Prozeduren zur Erkennung von aktuellen Sicherheitsproblemen und überwacht Desktop-PCs, Server, Anwendungen und intelligente Komponenten wie etwa Router oder VoIP-Geräte. Die Greenbone-Lösung ist inzwischen eine wichtige Sicherheitskomponente in über 30.000 professionellen Installationen und Integrationen quer durch alle Branchen und Unternehmensgrößen. Die Greenbone Vulnerability Management Software wurde bereits mehr als 2,5 Millionen Mal heruntergeladen.

Weitere Informationen unter **greenbone.net**
Folgen Sie uns auf Twitter: **twitter.com/GreenboneNet**