Wo helfen, wenn es nur röchelt?

Notrufnummern Wie funktioniert die Lokalisierung von Notrufen in Zeiten der Internettelefonie? Es ist eine Frage der Technik, aber auch des Rechts.

HANS-PETER SCHMOCKER

Der Wandel hin zur Internettelefonie stellt die Grundversorgung von Notrufen vor Herausforderungen. Der Bundesrat hat deshalb das Fernmeldegesetz per 1. Januar 2021 angepasst. Bevor die Verordnungen aber greifen können, müssen dafür die technischen Voraussetzungen geschaffen werden.

Wer Hilfe in einer Notsituation benötigt, hat von Gesetzes wegen das Recht, über eine Notrufnummer mit der sachlich und örtlich zuständigen Stelle verbunden zu werden. Deshalb sind Telekom-Anbieter dazu verpflichtet, die dafür notwendigen technischen Voraussetzungen zu schaffen. So betreibt die Swisscom als Grundversorgerin eine zentrale Datenbank, in welche die Telekomanbieter bei jedem Notruf die aktuellen Standorte ihrer Kunden und Kundinnen ablegen. Diese Standorte können dann von der Polizei, Ambulanz oder Feuerwehr abgefragt werden.

Das Recht auf Hilfe rechtlich neu regeln

Dieser Service besteht seit Anfang der 1970er Jahre. Damals beschränkte er sich dem technologischen Stand entsprechend auf die Weitergabe der genauen Adresse des Festnetzanschlusses. Mit dem Aufkommen der Mobiltelefonie wurde der Dienst erweitert, sodass die Notrufleitstellen bei Handy-Anrufen vom Netzbetreiber die Position der notleidenden Person aufgrund der Antennendaten übermittelt bekommen.

Intersys hat als Entwickler diese Datenservices für die schweizweiten Notrufe über Festnetz und mobile Verbindungen realisiert und seinen Dienst laufend den technologischen Anforderungen angepasst. Mit dem weiteren Wandel der Telefonie hin zu internetbasierten Services (Stichwort All-IP, Voice-over-IP) stand damit der Regulator vor der Herausforderung, das Recht auf Hilfe in Not auf eine neue gesetzliche Grundlage zu stellen. Denn mit den Möglichkeiten des Internets werden Notrufe durch Telefoniedienstanbieter ermöglicht, die ihren Telefondienst unabhängig von den Netzinfrastrukturanbietern betreiben.

Dies hat zur Folge, dass Notrufe viel schwieriger zu lokalisieren sind. Daher geht es zunächst einmal darum, sich auf technologische Standards zu einigen, damit Serviceanbieter für Telefonie und Internet sowie die Notruforganisationen mit den unterschiedlichen Szenarien eines Notrufs

Kundinnen und Kunden müssen keine Anwendung installieren oder anderweitig aktiv werden.

umgehen können. Denn zu den Standortinformationen von Festnetz- (mittlerweile All-IP) und Mobilanrufen der Mobile-Standards 3G, 4G und 5G gesellen sich unterdessen Anrufe über Voice-over-IP-Anlagen, Firmennetze, VoWifi (Voice-over-Wifi/WLAN) und nicht zuletzt das von der EU seit 2018 für neue Autos und leichte Nutzfahrzeuge vorgeschriebene Notrufsystem.

Die Standardisierungsinitiativen laufen unter dem Stichwort NG112 (Next Generation 112) in Europa und NG911 in den USA. 112 ist in Europa die einheitliche Nummer für sämtliche Arten von Notrufen. Wie andere Länder auch betreibt die Schweiz für die verschiedenen Blaulichtorganisationen noch andere Notrufnummern wie 117, 118, 143, 144, 145, 147, 1410, 1414 und 1415.

GPS zur besseren Lokalisierung

Eine Lösung für diese zum Teil schwierige Lokalisierung der Ortungsdaten des oder der Notrufenden bestünde in der Verwendung der gerätebasierten Lokalisierungsfunktionen, mit denen die Standortinformationen zum Beispiel des GPS (Global Positioning System) gleichzeitig mit dem Anruf an die Leitstelle weitergeleitet würden. Das könnte eine genauere Positionierung bei Mobilfunkanrufen ermöglichen, als es allein mit Antenneninformationen möglich ist.

Dabei wäre die automatische Verwendung der AML-(Advanced-Mobile-Location-)Applikation naheliegend, die von Google bei Android-Smartphones ab Version 9.0 und von Apple bei iPhones ab iOS 11.3 automatisch mitgeliefert wird. Kunden und Kundinnen müssten also keine Anwendung installieren oder anderweitig aktiv werden. Sobald sie die Notrufnummer 112 wählen, würde der Standortdienst (GPS) im Smartphone automatisch aktiviert, die genaue Position zum Beispiel mittels GPS ermittelt und via SMS übermittelt.

AML-System kommt doch

Diese GPS-Standortinformationen könnten nun zusätzlich zu den bereits beschriebenen Antenneninformationen in eine Datenbank mitübertragen werden und so eine genauere Lokalisierung ermöglichen. Im revidierten Fernmeldegesetz schreibt denn auch der Bundesrat in der neuen Verordnung vor, dass gerätеeigene Ortungsfunktionen bei einem Notruf auch ohne ausdrückliche Zustimmung des Kunden aktiviert werden dürfen und, soweit es die Technik zulässt, danach wieder deaktiviert werden sollen.

Konkret müssen demnach Mobilfunkanbieter bei Notrufen, bei denen die geräte- und betriebssystemeigene Ortungsfunktion sowie die sprachkanalunabhängige Übertragung der Standortinformation (eben mittels AML) genutzt werden, die Standortinformationen bereitstellen. Als Nachteil ist stellt sich nun aber heraus, dass Roaming-Szenarien noch nicht abschliessend geklärt sind.

Entsprechend sieht die Swisscom bei der AML-Regelung des Bundesamtes für Kommunikation (Bakom) «wesentliche Nachteile und Risiken». In einer Stellungnahme schrieb das Unternehmen im März 2020 im Hinblick auf die Vernehmlassung der neuen Verordnungen, der Mobilnetzbetreiber könne zu keinem Zeitpunkt die Verfügbarkeit und die Korrektheit der bereitgestellten Informationen gewährleisten oder plausibilisieren. Es sei wenig sachgerecht und überdies fragwürdig, wenn der Netzbetreiber für die ausserhalb seines Einflussbereichs liegenden Standortinformationen in die Pflicht genommen werde.

Die Swisscom hatte daher beantragt, die Fernmeldedienstverordnung zu ändern – vergeblich. Sie schlug vor, dass der Netzbetreiber nur für die Übertragung zuständig sei, die Entgegennahme und Auswertung der AML-Daten jedoch durch die zuständige Notrufzentrale direkt zu erfolgen habe. Eine solche dezentrale Lösung, wie sie beispielsweise bereits in Deutschland und Österreich zum Einsatz kommt, würde es den Leitstellen erlauben, die Daten direkt vom Mobilfunkkunden in einer eigenen Software zu empfangen und weiterzuverwenden.

Derzeit beste Lösung

Es ist nachvollziehbar, dass die Swisscom sich daran stört, gesetzliche Anforderungen zu erfüllen, für deren Einhaltung sie auf ein Fremdsystem angewiesen ist. Dennoch dürfte nach der Umsetzung der Bakom-Vorgaben die Standortgenauigkeit trotz den sich ändernden technologischen Voraussetzungen bei einem Teil der Fälle künftig verbessert werden, weil Notleidende mit GPS auf wenige Meter genau lokalisiert werden können. Bis dem allerdings so ist, wird es noch eine Weile dauern. Denn das revidierte Gesetz ist zwar seit 1. Januar 2021 in Kraft. Die technischen Anpassungen werden aber noch einige Zeit in Anspruch nehmen.

Ziel wird es sein, die unterschiedlichen Ortungsmethoden (Antennendaten, private IP-Adressen, Anschluss- und Infrastrukturdaten, Geodaten, gerätebasierte GPS-Daten und so weiter) zusammenzuführen. Intersys ist bereits mit der Swisscom dabei, einen zentralen Location-Information-Service zu entwickeln, dem die Informationen aller Systeme angeliefert werden. Ähnlich der jetzigen Notrufdatenbank werden die Notrufleitstellen bei einem mobilen Anruf bei diesem neuen Service den wahrscheinlichsten Standort des oder der Notleidenden abfragen können. Einmal fertiggestellt, dürfte dieser Service noch während einiger Zeit parallel zur heutigen Notrufdatenbank betrieben werden, bevor er sie vollständig ablösen wird.

Hans-Peter Schmocker, Product Manager Location Services, Intersys, Zuchwil.

Offline-Backups: Wichtig für die Verfügbarkeit im Falle von Ransomware-Angriffen. Im Bild: Leeds Castle in der Grafschaft Kent (GB).

Lernen aus dem Krisenfall

Microsoft Exchange Hack Der verbreitete Mailserver ist Angriffswellen ausgesetzt – ein guter Moment für einen Check im Unternehmen.

RALPH HUTTER

Am 2. März hat Microsoft in einem ausserordentlichen Sicherheits-Update vier bislang unbekannte Schwachstellen für Microsoft Exchange Server geschlossen, die in verschiedenen aktuellen Angriffen genutzt werden. In der Schweiz sind laut dem Nationalen Zentrum für Cybersicherheit (NCSC) mehrere hundert Organisationen betroffen. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) ruft Stufe drei, «orange», aus und schätzt Zehntausende von betroffenen Systemen alleine in Deutschland. Weltweit müssen Hunderttausende Organisationen ihre Infrastruktur updaten, um die Sicherheitslücke wirksam zu schliessen. Angriffsziele sind nicht Privatanwender von E-Mail-Diensten, sondern Organisationen, die einen eigenen Exchange-Mailserver der Versionen 2013, 2016 und 2019 betreiben. Die Cloud-Versionen von Microsofts E-Mail-Service wie Office 365 sind nicht betroffen.

Meist staatlich motivierte Angriffe

Nach Angaben von Microsoft richteten sich die Angriffe ursprünglich gegen Forschungseinrichtungen mit Pandemie-Bezug, Universitäten, Anwaltskanzleien sowie Firmen im Rüstungsbereich und NGO. Diese Vorfälle werden einer staatlichen Hackergruppe aus China, Hafnium genannt, zugeordnet. In jedem Fall handelt es sich um hochqualifizierte und raffinierte Akteure, die verschiedene, langjährige Schwachstellen geschickt zu einer neuen Angriffsform kombinieren. Zuerst wird der Zugang zum Mailserver über gestohlene Passwörter oder die Zero-Day-Schwachstellen erlangt. Darauf kann eine webbasierte Kommandozeile eingerichtet

Das Ziel der Angreifer ist es, möglichst lange unentdeckt zu bleiben und permanenten Zugang zu erhalten.

werden, über die der Server aus der Ferne administriert und Daten abgegriffen werden können.

Diese Form eines Angriffs heisst APT (Advanced Persistent Threat). APT sind lang andauernde, komplexe und spezifische Angriffe auf KMU, Grossunternehmen, Behörden oder auch kritische Infrastrukturen. Typischerweise handelt es sich nicht um einen schnellen Hack. Das Ziel der Angreifer ist es, möglichst lange unentdeckt zu bleiben und permanenten Zugang in das kompromittierte System beziehungsweise das Unternehmen zu erhalten. Wegen der Komplexität und dem erforderlichen Know-how sind dies meist staatlich motivierte Angriffe zur Industriespionage oder politischen Einflussnahme.

Mit der Bekanntmachung der Sicherheitslücken haben sich kurzfristig mindestens zehn weitere Hackergruppen dazugesellt, die mit automatisierten Attacken die verwundbaren Systeme nun auf breiter Front angreifen. Sie sind Trittbrettfahrer. Sie spekulieren darauf, dass auch nach Verfügbarkeit der Sicherheits-Updates weiterhin Tausende Systeme ungepatcht bleiben, da insbesondere kleine und mittelständische Unternehmen die aktuellen Sicherheitslücken noch während Wochen nicht beheben werden.

Wenn der Chef zur Zahlung auffordert

Das eröffnet das Feld für weitere Cyberstraftaten wie Data Leaks als Basis für zum Beispiel Erpressung von Lösegeldforderungen, die Installation von Krypto-Mining-Malware oder auch schlicht die Übernahme eines E-Mail-Kontos, um beispielsweise im Namen des Geschäftsführers Zahlungsanweisungen an die Buchhaltung zu senden, den sogenannten CEO Fraud. Die Situation wird sich damit auf absehbare Zeit nicht entschärfen.

Der Hersteller, aber auch verschiedene nationale CERT (Computer Emergency Response Team) wie in der Schweiz das Nationale Zentrum für Cybersicherheit haben detaillierte Handlungsanweisungen für die Behebung der Schwachstellen publiziert. Doch dies sind ausschliesslich technische Antworten auf eine spezifische Schwachstelle. Und die nächste kommt bestimmt.

Abseits der Technik stellen sich wesentlich wichtigere Fragen. Nämliche solche von organisatorischer und IT-strategischer Natur. Sind im Unternehmen überhaupt die erforderlichen Gremien wie CERT und Krisenstäbe vorhanden und einsatzfähig? Sind Notfallprozesse definiert, aktualisiert und geschult und ist das entsprechende Know-how vorhanden? Existiert ein Kommunikationskonzept, das im Falle eines Datenabflusses Informationen an Mitarbeitende, Kunden, Lieferanten und Behörden bereithält? Die Cyberkriminalität entwickelt sich in zunehmendem Tempo und es werden ständig neue Verwundbarkeiten und Angriffsmöglichkeiten veröffentlicht. Cyberkriminelle werden immer agiler. Sie nutzen neue Technologien blitzschnell aus, passen ihre Angriffe auf neuen Methoden an, kooperieren in Netzwerken und koordinieren komplizierte Angriffe innerhalb von Minuten.

Werden Unternehmen noch in der Lage sein, geschäftskritische Systeme selber sicher zu betreiben?

Erschwerend gesellt sich die Pandemiesituation dazu. Grosse Teile der Belegschaft arbeiten behelfsmässig im Homeoffice über private Infrastruktur, und auch bei einzelnen Geschäftsprozessen muss entsprechend improvisiert werden. Eine perfekte Ausgangslage für Cyberkriminelle.

Damit stehen der betroffene Exchange Server und diese Angriffswelle während Covid-19-Zeiten doppelt sinnbildlich dafür, ob ein Unternehmen künftig überhaupt noch in der Lage sein wird, geschäftskritische Systeme selber sicher zu betreiben und welche Fähigkeiten und Rollen im Unternehmen künftig benötigt werden, um dem nächsten Angriff widerstandsfähig zu begegnen.

Ralph Hutter, Director of Studies CAS Cyber Risk & Security, HWZ Hochschule für Wirtschaft Zürich, Zürich.

Die Schweiz ist auf Kurs

Fertigungsindustrie Sie nutzt zunehmend die Chancen der Digitalisierung. Ein Grossteil der Unternehmen hat Digitalisierungsprojekte angestossen.

ADRIAN MARTI

Zu Beginn sind Digitalisierungsbestrebungen oft durch operative Bedürfnisse getrieben. Damit lässt sich nicht nur rasch Nutzen generieren, sondern auch Wissen und Erfahrung im Unternehmen aufbauen. Empfehlenswert ist, von Anfang an auch die Cybersicherheit zu einem integralen Bestandteil dieser Digitalisierungsvorhaben zu machen.

Exemplarisch für den Werkplatz Schweiz nehmen Ricardo Nebot, Head of IT bei Emmi Schweiz, und Ralph Hecht, Head of IT von EAO, Stellung. Obwohl beide Unternehmen in unterschiedlichen Branchen tätig sind, zeigt sich, dass sie das Thema Cybersicherheit ziemlich ähnlich angehen.

Technik, Prozesse und Organisation

Der Aufbau von Cybersicherheit gelingt nicht von heute auf morgen und kann auch nicht per Dekret verordnet werden. Ziel muss es sein, sie auf allen Ebenen stufengerecht als Element zu etablieren, das stets in die Geschäftsentscheidungen einbezogen wird. Ein im Unternehmen verankertes Management der Cybersicherheit sollte die drei Ebenen Technik, Prozesse und Organisation umfassen.

Eine von AWK Mitte 2020 bei rund hundert Entscheidungsträgern aus grossen und mittelgrossen Unternehmen durchgeführte Studie zeigt ein durchzogenes Bild in Bezug auf den Stand der Informationssicherheit. Cybersicherheit wird zwar von 70 Prozent der befragten Unternehmen als Voraussetzung für professionelles Handeln und teilweise sogar als Differenzierungsmerkmal wahrgenommen. Gleichzeitig sehen sich aber lediglich 20 Prozent der Befragten als ausreichend gerüstet für den Erhalt eines angemessenen Sicherheitsniveaus. Auch aus der Umfrage der Arbeitsgruppe «Digitalstrategie» von Industrie 2025 unter Co-Leitung von AWK im vergangenen Herbst geht hervor, dass nur jedes fünfte der 113 befragten Unternehmen grosse Investitionen in Sicherheitstechnologien tätigt.

Ricardo Nebot von Emmi Schweiz hat eine klare Meinung: «Die Diskrepanz lässt sich auch dadurch erklären, dass die heutigen Angriffsszenarien vielfältiger und professioneller geworden sind und deren effektive Bekämpfung Unsummen verschlingen kann. Vieles, was wir heute noch nutzen, basiert auf alten Technologien. Dazu gehören beispielsweise die verwendeten Protokolle, die aus Zeiten stammen, in denen die heutigen Angriffsmöglichkeiten noch undenkbar waren.»

Ralph Hecht von EAO betrachtet diesen Aspekt ebenfalls aus einer technischen Perspektive: «Produktionsumgebungen sind primär nicht auf Sicherheit ausgelegt, sondern auf Funktionalität und beinhalten keine ‹Security by Design›. Auch Lifecycles wie bei Standard-Applikationen können hier nicht berücksichtigt werden.»

Ein risikobasierter Ansatz

Beim Aufbau und Erhalt der Cybersicherheit bewährt sich ein risikobasierter Ansatz für das Management von Informationsrisiken. Hierzu müssen sowohl der Risikoappetit des Unternehmens identifiziert als auch die Ownership der Risiken definiert werden. Eigner der Risiken ist typischerweise die Linie. Diese finanziert direkt oder indirekt auch die Massnahmen zur Mitigation der Risiken.

Es ist daher empfehlenswert, die Auswirkungen auf das Business in den Fokus der Risikodiskussion zu stellen und Betroffene zu Beteiligten zu machen. Die Verfahren zur Identifikation, Messung und Bewertung der Risiken sollten sinnvoll und nachvollziehbar ausgestaltet werden, damit ein Mehrwert für das Unternehmen generiert werden kann und der Umgang mit den vorhandenen Risiken von allen getragen wird.

Ricardo Nebot sieht dies ganz pragmatisch: «100-prozentige Sicherheit ist eine Illusion, speziell bei der Vielzahl von Dienstleistern, mit denen man heute vernetzt ist. Viel wichtiger ist, die Risiken richtig abzuwägen, die Kronjuwelen zu identifizieren und zu schützen sowie den Spagat zwischen bestmöglichen Services und maximaler (bezahlbarer) Sicherheit zu schaffen.»

Ein hohes Gewicht hat heutzutage auch die Beurteilung von Drittrisiken. In der IT kommt heute kaum noch ein Unternehmen an Cloud-Lösungen vorbei. Für IT und auch für operationelle Technologien (OT) wie zum Beispiel Maschinensteuerungen in der Produktion ist der Zugriff von aussen für beispielsweise die Fernwartung heutzutage gang und gäbe.

«Der unbekannte Faktor dabei ist die Sicherheit beim Lieferanten, der auf unsere Maschinen und Infrastruktur zugreift. Obwohl alles vertraglich geregelt ist, nützt uns das im Ereignisfall nicht viel. Das

Der unbekannte Faktor ist die Sicherheit beim Lieferanten. Vertragliche Regelungen nützen im Ereignisfall wenig.

macht uns zu einem gewissen Grad abhängig und fordert Vertrauen in die Professionalität und das Qualitätsversprechen unserer Partner. Gerade bei Cloud-Lösungen muss ich mich darauf verlassen können, dass die grossen Player am Markt einiges mehr in die Sicherheit ihrer Lösungen investieren, als wir uns leisten können oder wollen», sagt Hecht.

Bedrohungen und Firmen ändern sich

Vertrauen ist gut, Kontrolle ist besser, sagt ein Sprichwort. Leider sind gerade bei den ganz grossen Anbietern Kontrollen nahezu unmöglich. Es finden sich zwar oft anerkannte Zertifizierungen oder Service Organization Control Reports nach Standard 2 oder 3. Doch auch hier müssen die Kunden darauf vertrauen, dass diese akkurat sind. Es empfiehlt sich daher, die eigenen Sicherheitstechnologien und -mechanismen regelmässig zu überprüfen, sie auf dem neuesten Stand zu halten und zu testen. Denn im Zeitalter der Digitalisierung verändern sich sowohl die Bedrohungen als auch die Unternehmen selbst kontinuierlich.

Ein harmonisches Zusammenspiel aller Faktoren setzt eine ausgewogene Mischung aus Mensch und Technologie voraus. Verwaltungsräten ist zu empfehlen, sich als Sparringspartner des Managements zu positionieren und sich aktiv in die Diskussion zum Risikoappetit einzubringen. Die IT sollte sich nicht nur als Betreiber der IT-Landschaft sehen, sondern als aktiver Ansprechpartner der Linie, um gemeinsam die optimalen Lösungen zu finden. Hinsichtlich der Entwicklung und Förderung einer sicherheitsbewussten Organisation sind sich Nebot und Hecht einig: Awareness-Trainings auf allen Stufen sind ein zentraler Bestandteil, um die definierten Sicherheitsziele erfolgreich zu erreichen. Ralph Hecht: «Mein Ziel ist ‹Security by Default› – in der Technik ebenso wie in der Organisation.»

Adrian Marti, Partner im Bereich Cyber Security & Privacy, AWK Group, Zürich.