Die ersten Sekunden entscheiden

Sicherheit im Auto Aus einem Unfall hat G4you eine Lösung kreiert: Eine Hochleistungskamera filmt die kritischen Sekunden. Das könnte Kosten senken.

ECKHARD BASCHEK

Caroline Bono ist passiert, was sich niemand wünscht – ein Autounfall mit bleibenden Schäden. Das Zynische dabei war, dass man bei der Unfallaufnahme nur spekulieren konnte, was ihr beim Aufprall alles zugestossen war. Von aussen ist das nur schwer erkennbar, denn trotz offensichtlichen Symptomen wurde am Unfalltag kein MRT des Rückens und des Hirns veranlasst.

Hätte man beim Unfall sozusagen zusehen können, hätte sich Caroline Bono nicht nur viel Leid ersparen können, es hätten sie auch die Versicherungen anders unterstützen können – ganz abgesehen vom langjährigen Schaden durch den Arbeitsausfall der Rechtsanwältin.

Arbeitsunfähigkeit verhindern

Es ist bei Autounfällen beispielsweise nicht bekannt, ob, mit welcher Kraft und in welche Richtung die Körperbewegung stattgefunden hat oder ob beispielsweise durch eine nicht symmetrische Sitzhaltung auch andere Torsionskräfte an den Insassen aufgetreten sind. Das wiederum hat zur Folge, dass Verletzungen oft übersehen und nicht optimal behandelt werden.

Studien belegen laut Caroline Bono, dass nach Verkehrsunfällen 67 Prozent aller Halswirbelbrüche, 45 Prozent aller Subluxationen und 66 Prozent der Kopfverletzungen mit herkömmlichen Diagnose- und Röntgenverfahren in der Notaufnahme übersehen werden. Bestimmte Läsionen wie zum Beispiel Mikroeinblutungen, die wertvolle Hinweise geben würden, können nach wenigen Tagen wieder verschwunden sein, und die Abklärungen zu den Spätfolgen erfolgen oft erst Wochen später – zu spät. Das hat zur Folge, dass Unfallopfer arbeitsunfähig bleiben, obwohl man sie mit der richtigen Behandlung hätte wiederherstellen können.

Derzeit gibt es keine Produkte, die Unfälle in Echtzeit dokumentieren.

Aus der Not eine Tugend gemacht

Derzeit gibt es keine Produkte auf dem Markt, die Unfälle in Echtzeit dokumentieren. G4you ist nun daran, einen Prototyp zu entwickeln: Die Aufzeichnungen von rund dreissig Sekunden einer Hochgeschwindigkeitskamera werden bei einem Aufprall nicht mehr überschrieben, sondern an einen Server gesendet, damit die Rettungskräfte und die Notfallmediziner schnell sehen, was genau passiert ist. Gemäss der Planung von G4you – dahinter stehen die Juristin und ihr Ehemann Ruedi Rothenbühler, ein erfahrener Allgemeinmediziner, sowie ein Team von Beratern – könnten diese Kits in Neuwagen und Occasionen eingebaut werden. Caroline Bono hat dazu nun ein Crowdfunding lanciert (siehe Interview rechts), um den Prototyp realisieren zu können. Sie arbeitet dazu mit dem Switzerland Innovation Park Biel/Bienne zusammen. Zuständig ist Elektroingenieur Felix Kunz, CEO und Co-Founder des Parks. Was sagen Mediziner dazu? Auf Anfrage erklärt Ludwig Theodor Heuss, Chefarzt Innere Medizin – mit einem Schwerpunkt auf die Umsetzung betriebswirtschaftlicher und gesundheitsökonomischer Konzepte in die Praxis – sowie Verantwortlicher für Notfälle am Spital Zollikerberg: «Idee und Konzept sind bestechend. Es wäre hilfreich, wenn man diese zusätzlichen Daten hätte.» Harald C. Gall, Professor für Software Engineering der Uni Zürich, meint: «Die Technologie dazu steht bereit, wir können sie jetzt zum Wohl der Verletzten einsetzen.»

www.g4you.org

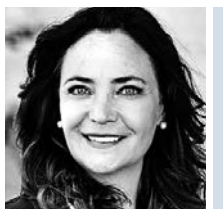
GETTY IMAGES

Bring Your Own Device (BYOD): Wichtig sind Anweisungen für den Umgang mit den Geräten. Im Bild: Bourtange, eine bewohnte ehemalige Festung in den Niederlanden, Provinz Groningen.

«Wir brauchen noch 1,5 Millionen Franken»

Wie viel Geld haben Sie schon eingesetzt und wie viel brauchen Sie?
Caroline Bono: Konkret stecken jetzt schon über 200 000 Franken in dem Projekt, ohne die indirekten Kosten. Wir müssen nun möglichst schnell einen Prototyp entwickeln, um zu beweisen, dass man die Lösungsidee in die Tat umsetzen kann – auch damit die Autohersteller und Versicherungen den Nutzen klar erkennen können. Dazu fehlen jetzt noch geschätzte 1,5 Millionen Franken innerhalb der nächsten zwei Jahre.

Stichwort IT-Sicherheit: Wie stellen Sie sicher, dass keine unerwünschten Personen an heikle Daten gelangen?
Die Daten werden verschlüsselt an bestimmte Server weitergeleitet, der Kreis ist also stark eingeschränkt. Zudem gehören die Aufnahmen rechtlich gesehen immer den Opfern, und alle involvierten Parteien müssen das auch vertraglich bestätigen.



Caroline Bono
Anwältin und Coach, G4you

In Teslas werden schon länger Kameras verbaut. Warum braucht es Ihre Lösung noch?
In einigen modernen Elektroautos gibt es zwar Kameras und auch Übertragungslösungen, aber für eine gute Analyse von Unfällen braucht es Hochgeschwindigkeitskameras, die ausserdem von tiefen Minustemperaturen bis zu hohen Temperaturen im Sommer im Fahrzeug zuverlässig funktionieren. Und für Occasionsfahrzeuge gibt es nicht einmal das.

Was heisst eigentlich G4you?
Es steht für «Guardian Angel for You», also für die Verletzten.

Sie haben über Ihren Unfall und die Widrigkeiten mit der Erstversorgung und den Versicherungen ein Buch publiziert, «Allein gegen Goliath: Wie mein rundumversichertes Leben zum Albtraum wurde». Wollen Sie mit G4you nicht auch Ihr Trauma verarbeiten?
Das ist sicher so. Aber im Wesentlichen wollen wir anderen mein Schicksal ersparen und etwas Gutes aus der Sache machen.

INTERVIEW: ECKHARD BASCHEK

Es einfach zu machen, ist nicht einfach

Datensicherung Mit der Vervielfachung der Kommunikationskanäle muss die Verschlüsselung und Entzifferung einfach zugänglich bleiben.

ANDREAS KUTTER

Opfer einer Cyberattacke zu werden, gehört für viele Schweizer Unternehmen mittlerweile zum Alltag. Regelmässige Studien des Beratungsunternehmens KPMG zeigen, dass in der Schweiz mehr als die Hälfte der von Cyberangriffen betroffenen Unternehmen ihren Geschäftsbetrieb unterbrochen haben und etwas mehr als ein Drittel dadurch einen finanziellen Schaden erlitten hat. In Frankreich hat sich die Zahl der Computerangriffe auf Unternehmen und Dienste seit Beginn der Pandemiekrise vervierfacht.

Sanitas Troesch, Swatch, Amag, Stadler

Das Beispiel des zum französischen Saint-Gobain-Konzern gehörenden Bad- und Küchenspezialisten Sanitas Troesch, der einer weltweiten Cyberattacke zum Opfer fiel, bleibt im Gedächtnis haften. In jüngster Zeit wurden die Swatch Group, die Amag Group und Stadler Rail hart getroffen.

Natürlich hat sich in den letzten zwanzig Jahren in Bezug auf die IT-Sicherheit viel verändert. Ein wichtiger Aspekt ist die weit verbreitete Nutzung von Cloud Computing, sowohl für die Datenspeicherung als auch für den Zugriff. Dies hat einen enormen Einfluss darauf, wie Cybersicherheitsfragen angegangen werden müssen. In den frühen 2000er Jahren war die Idee, eine Art Mauer um das Unternehmen zu errichten.

Im Jahr 2021 ist der Ansatz ein ganz anderer: Der Zugriff auf die Daten kann sowohl vom Unternehmen als auch von zu Hause oder von unterwegs aus erfolgen. Die Daten werden daher teils auf den Servern des Unternehmens, teils in der Cloud und manchmal sogar auf den privaten Computern der Mitarbeitenden gespeichert.

Hacker sind keine isolierten Einzelpersonen mehr, sie agieren in Netzwerken, als kriminelle Organisationen.

Als logische Folge vergrössert diese Flexibilität auch drastisch die Angriffsfläche, die potenziell von Hackern ausgenutzt werden kann.

Eine Tendenz zur Datensicherung

Wir müssen umso wachsamer sein, als Hacker heute viel raffinierter agieren als in der Vergangenheit: Hacker sind keine isolierten Einzelpersonen mehr, die sich hinter ihren Computern verschanzen, sondern agieren zunehmend in Netzwerken; als kriminelle Organisationen.

Die Frage ist, ob sich ein Unternehmen noch vollständig gegen Eindringlinge schützen kann. Anstatt zu versuchen, die gesamte IT-Umgebung eines Unternehmens zu schützen, besteht eine Lösung darin, die Daten selbst zu sichern. Um es bildlich auszudrücken: In der Vergangenheit hat man versucht, eine Art Zaun um das Unternehmen zu ziehen. Jetzt wissen wir, dass der Zaun Löcher hat – also werden wir uns mehr darauf konzentrieren, den Zugriff darauf zu kontrollieren, basierend auf dem Ort, an dem er sich befindet, mittels Verschlüsselungs- und Autorisierungslösungen.

Doch heute tauschen sich die Menschen mit ihren Arbeitgebern über ihre berufliche E-Mail, über Messaging-Dienste wie Whatsapp oder per Chat aus. Es stellt sich daher die Frage, ob die Vervielfachung dieser Kommunikationskanäle die Sicherheitslage verkompliziert. Dies bringt uns zurück zur Frage, was gesichert werden soll. Sollen wir die Kanäle sichern, über die diese Daten verteilt und abgefragt werden, oder eher die Daten selbst? Heute geht der Trend zur Sicherung der Daten selbst.

Das Beispiel von Postfinance ist aufschlussreich. Dieses Unternehmen bietet nun sowohl mobile Bankdienstleistungen als auch zertifizierte Zahlungssysteme wie Twint an. Auch wenn einige traditionelle Institutionen derzeit von Fintechs herausgefordert werden, bleiben die wesentlichen Punkte, die es zu schützen gilt, dieselben: Es geht vor allem darum, die Sicherheit von Finanztransaktionen zu gewährleisten. Denn im Gegensatz zu anderen Branchen besteht die Herausforderung nicht nur darin, die Daten allgemein zu schützen, sondern auch darin, die korrekte Durchführung der Finanztransaktion sicherzustellen.

Es gibt einfache Lösungen, um Probleme während der Entschlüsselungsphase zu vermeiden.

Verschiedene Risiken müssen vermieden werden: Eine Transaktion kann auf einen Dritten umgeleitet werden, ihr Betrag kann verändert werden. Aus all diesen Gründen müssen die mit einer Transaktion verbundenen Daten mit Verschlüsselungstechniken geschützt werden. Bei diesen Systemen wird jedoch oft gesagt, dass es zwei Arten von Risiken gibt: erstens, dass die Verschlüsselungslösung zu einfach ist; zweitens, dass der Benutzer die Entschlüsselung nicht beherrscht.

Die Postit-Zettel-Gefahr

Deshalb ist die Entschlüsselung immer etwas, das gefürchtet wird. Dennoch gibt es einfache Lösungen, um Probleme während der Entschlüsselungsphase zu vermeiden. Der Entschlüsselungsschlüssel kann zum Beispiel in vier oder fünf Teile aufgeteilt werden, die an verschiedenen sicheren Orten gespeichert werden. Oder der Entschlüsselungsschlüssel kann an einem hochsicheren Ort abgelegt werden.

Das Wichtigste ist immer, dass die gewählte Lösung einfach ist, erklärt die Thales Group, Anbieter für Cybersicherheit und Datenschutz. Wenn Benutzer aufgefordert werden, ein 32-stelliges Passwort mit Klein- und Grossbuchstaben und Sonderzeichen zu verwenden, ist die Wahrscheinlichkeit gross, dass sie das Passwort auf einen Postit-Zettel schreiben, der neben ihrem Computer liegt. Besser ist es, ein Passwort zum Beispiel in Form einer Phrase zu verwenden, die man sich leichter merken kann, oder eine Zwei-Faktor-Authentifizierung zu nutzen.

Andreas Kutter, Geschäftsleiter Deutsche Schweiz, Kyos, St. Gallen.
www.kyos.ch