Live aus dem Krankenhaus

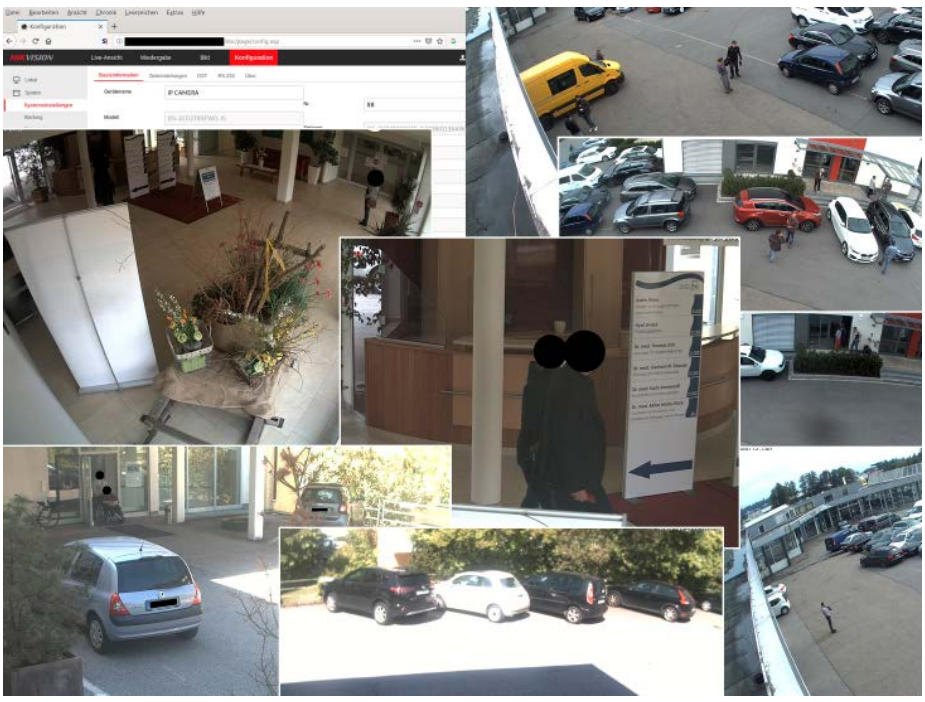
Ungeschützte Linksammlung leakt Überwachungsaufnahmen

Wenn man sich von einem Fachbetrieb Überwachungskameras installieren lässt, sollte man auf der sicheren Seite sein. Bei einem Elektroinstallationsbetrieb gab es aber eine folgenschwere Panne: Ein Intranet-Server mit URLs und Zugangsdaten gab Live-Aufnahmen einer Klinik und mehrerer Firmen für jedermann preis.

Von Mirko Dölle und Joerg Heidrich

Wer als Patient die Klinik am Isar Park in Plattling in Bayern betrat, hatte ein potenziell weltweites Publikum: Egal ob Notaufnahme oder Haupteingang, Empfang oder Besucherparkplatz, alles wird von Kameras überwacht – und deren Aufnahmen waren live für jedermann abrufbar. Denn jede einzelne der mehr als ein Dutzend IP-Kameras auf dem Klinikgelände ist per DynDNS-Dienst und Portfreigabe direkt aus dem Internet zu erreichen.

Die Adressen und die für den Zugriff notwendigen Login-Daten waren ungeschützt auf einem Webserver des mittelständischen Elektroinstallationsbetriebs ELAB Elektroanlagenbau GmbH aus Deggendorf einsehbar, der für die Installation der Überwachungssysteme verantwortlich zeichnet. In der Übersicht fanden sich auch mehr als ein Dutzend weitere Links zu Kameras einer Baufirma, eines Autohauses, einer Wohnanlage in Kreut sowie etlichen Baustellen und anderen Orten in der Region. Praktischerweise waren die Anmeldedaten gleich in den Links integriert – ein Klick genügte, um sich live die Überwachungsaufnahmen anzusehen.



Die Auflösung und die Ausrichtung der Kameras im Eingangsbereich und vor der Notaufnahme der Klinik erlauben es, sogar Personen und Kennzeichen von Fahrzeugen zu erkennen. In einem Fall bekamen wir sogar Admin-Rechte zum Überwachungssystem.

Offen für alles

Im Fall der sogenannten Maurerhalle der Baufirma aus Deggendorf war sogar der Admin-Zugang zum Überwachungssystem hinterlegt, das zugehörige Passwort wurde an Trivialität nur von denen der anderen Überwachungskameras übertroffen: Sie folgten stumpf dem Muster 113355. Auch den Benutzernamen hätte man leicht erraten können, wenn er nicht ohnehin auf der Übersichtsseite gestanden hätten.

Bei den meisten der aufgelisteten Überwachungskameras handelt es sich um Mobotix M10, die mit zwei Objektiven ausgestattet sind und hochauflösende Bilder mit bis zu 1280 × 960 Pixeln bieten. Die nötigen Informationen, um auf diese Bilder zuzugreifen, findet man im Handbuch der Kamera. Die Qualität der Aufnahmen ist völlig ausreichend, um bei der Notaufnahme, dem Krankenhausparkplatz und dem Schwesternwohnheim der Klinik am Isar Park Kennzeichen von PKW zu entziffern oder Personen zu erkennen. Am Empfang direkt neben dem Haupteingang gibt es eine weitere Kamera für Nahaufnahmen des Tresens.

Die Links auf der Übersichtsseite legen nahe, dass außerdem der Zugang, die Schaukel und die Fensterfront des Kindergartens von weiteren Kameras überwacht werden, die während unserer Recherchen allerdings nicht in Betrieb waren. Das Café und die Raucherecke konnten wir hingegen aus der Ferne besichtigen. Bei der Wohnanlage in Kreut ist die Kamera so hoch angebracht, dass man mit ihr von oben auf etliche Balkons der Nachbarschaft und mitunter bis in die Wohnzimmer blicken konnte.

Videoüberwachung in der DSGVO

Aus datenschutzrechtlicher Sicht haben sowohl das Unternehmen ELAB als auch die Firmen und Organisationen, die des-

sen Leistungen zur Videoüberwachung beauftragt haben, offenbar eine ganze Menge falsch gemacht. Das fängt bereits damit an, dass die Bilder der Kameras auf keinen Fall offen ins Netz gestellt werden dürfen. Hierbei dürfte es sich um einen Vorfall handeln, der nach Artikel 33 der DSGVO an die Behörden zu melden ist.

Doch viel weitergehend stellt sich die Frage, ob die Kameras diese Stellen überhaupt überwachen dürfen. Zwar ist Videoüberwachung in der DSGVO nicht explizit geregelt. Auch im ergänzenden deutschen Bundesdatenschutzgesetz finden sich in Paragraf 4 nur Vorschriften für öffentlich zugängliche Räumlichkeiten. Dennoch stellt das dauerhafte Filmen eine Datenverarbeitung dar, die nur unter den engen Voraussetzungen des Datenschutzes zulässig ist.

Voraussetzung dabei ist, dass öffentlich zugängliche Bereiche per Kamera beobachtet werden und dies nicht ausschließlich zu privaten Zwecken geschieht. In diesem Fall ist das Betreiben von Kameras gemäß Artikel 6 DSGVO nur dann zulässig, wenn dies „zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist". Allerdings muss im Rahmen einer Interessenabwägung darauf geachtet werden, dass die entgegenstehenden Interessen der betroffenen Personen, hier also der Beobachteten, diesem Interesse nicht überwiegen.

Wird also nur das eigene, nicht von Dritten genutzte Grundstück überwacht, steht dem grundsätzlich rechtlich nichts entgegen. Diese Maßnahme ist in aller Regel von der Wahrnehmung des Hausrechts gedeckt. Dieses Recht endet aber dort, wo auch regelmäßig Dritte von der Videoüberwachung betroffen sind, also an den Grundstücksgrenzen. Öffentlicher Raum, also etwa Gehwege oder Straßen und das Grundstück des Nachbarn, sind bei der Überwachung tabu.

Beschilderungspflicht

Im Falle der Firma ELAB wurden jedoch massiv öffentlich zugängliche Bereiche überwacht – und mit der Nahaufnahme des Tresens, der Raucherecke oder der Notaufnahme sogar sensible Bereiche, in denen die sich dort aufhaltenden Personen kaum mit einer Überwachung rechnen müssen. Für die Überwachung dieser Bereiche wird der Klinikbetreiber sehr gute Argumente brauchen, um sie zu rechtfertigen. Es spricht alles dafür, dass hier die Interessen der Betroffenen gegenüber denen der Klinik überwiegen, sodass die Überwachung unzulässig ist. Darüber hinaus fordern die Datenschutzbehörden, dass an den jeweiligen Stellen durch eindeutige und unübersehbare Schilder auf die Videoüberwachung hingewiesen wird. Bei der Klinik am Isar Park befindet sich laut ELAB ein Schild an der Einfahrt zum Parkplatz. Auf diesem Schild muss etwa der Name der verantwortlichen Stelle ebenso vermerkt sein wie die Verarbeitungszwecke und die Rechtsgrundlage, die Dauer einer Speicherung der Aufzeichnung und die Angabe, welches berechtigte Interesse der Verantwortliche für den Betrieb der Kameras geltend macht.

Verantwortlicher im rechtlichen Sinn ist in den vorliegenden Fällen jeweils der Betreiber der Kameras, also das Krankenhaus, das Autohaus oder das Bauunternehmen. ELAB wird für diese Unternehmen als sogenannter Auftragsverarbeiter tätig gewesen sein, wofür zusätzlich ein gesonderter Vertrag notwendig ist.

Den Verantwortlichen, im vorliegenden Fall vor allem dem Krankenhaus, droht für die möglicherweise unzulässige Ausrichtung der Kameras und die möglicherweise fehlenden Hinweisschilder ein Bußgeld nach DSGVO. Tatsächlich gibt es im deutschen wie im europäischen Raum eine ganze Menge derartiger Strafen, die sich meist im vier- bis fünfstelligen Bereich bewegen. Ein weiteres Bußgeld droht für das Einspeisen der Kamerabilder in das Internet, welches – abhängig von den internen Vereinbarungen – ELAB treffen könnte.

Verkappte Datenhalde

Damit aber nicht genug: Nicht alle auf der Übersichtsseite aufgeführten Kameras waren direkt aus dem Internet zu erreichen, mitunter scheinen Aufnahmen insbesondere von diversen Baustellen auf dem Server von ELAB gespeichert worden zu sein – auf Jahre hinaus. Die älteste von uns vorgefundene Überwachungsaufnahme stammte aus dem Oktober 2016, ist also fast vier Jahre alt. Das wiederum wirft die Frage der Speicherfristen auf.

Diese orientiert sich bei Aufzeichnungen strikt am Grundsatz der Erforderlichkeit. Allerdings gehen die Datenschutzbehörden auch bei zulässiger Videoüberwachung in aller Regel von einer Speicherdauer von maximal 48 Stunden aus. Nach dieser Frist sind die Aufzeichnungen zu löschen, sofern nicht ausnahmsweise in dem überwachten Bereich etwas vorgefallen ist. Ausnahmen mag es hier im Bereich von Hochsicherheitstrakten geben, sicher aber nicht bei Raucherecken. Geht die Speicherung über den Zeitraum hinaus, so ist darin ein Verstoß gegen das Prinzip der Datensparsamkeit zu sehen. Auch hierfür wird es mit großer Wahrscheinlichkeit ein Bußgeld geben.

Nachdem wir ELAB per Fax informierten und um eine Stellungnahme baten – unsere zuvor versandten E-Mails kamen wohl nicht an –, ging es schnell: Nicht einmal 24 Stunden dauerte es, bis die Übersichtsseite offline genommen und die Kameras der Kunden mit neuen Zugangsdaten versehen waren. So soll es sein. Außerdem erhielten wir eine Stellungnahme des Geschäftsführers: Der Server mit der Kameraübersicht sollte nie öffentlich zugänglich sein, sondern nur zu Wartungszecken im Intranet zur Verfügung stehen. Es war also offensichtlich ein Konfigurationsfehler der Firewall, der das Datenleck eröffnete. Dies sei nun gestopft. Bei der in einer Wohnanlage installierten Kamera sei außerdem versäumt worden, die inzwischen bezogenen Häuser auszublenden, dies habe man sofort nachgeholt. Die für die Umstellung entstandenen Kosten trage ELAB und übernehme damit diesbezüglich die finanzielle Verantwortung.

Die Datenpanne müssen sich wohl die Admins von ELAB ankreiden lassen: Eine ungeschützte Übersichtsseite mit Zugangsdaten ist auch im Intranet ein No-Go, Trivial-Passwörter sind es ebenso. Die sichere Aufbewahrung individueller Passwörter für alle Kameras verursacht mehr Zeitaufwand bei der Einrichtung und somit höhere Kosten – ist aber letztlich viel billiger als jede Strafe, die die DSGVO vorsieht. *(mid@ct.de)* c't