Angriff aus heiterem Himmel

Diebstahl, Spionage, Sabotage – die Gefährdungslage von Unternehmen hat sich in den letzten Jahren dramatisch verschlechtert. In der öffentlichen Wahrnehmung dominiert zurzeit die Internet-Kriminalität. Doch die Täter kommen auch zu Fuß – oder aus heiterem Himmel.

Manfred Godek,
Produktion Nr. 05, 2023

Diebstahl, Spionage, Sabotage – Gefahren für Gewerbeimmobilien stecken nicht nur in der IT. Selbst Hacker machen sich inzwischen ‚physisch' an ihre Opfer heran, indem sie sich mittels Drohnen in die lokalen WLAN-Netze einklinken.
Bild: Kadmy - stock.adobe.com

Monheim (sm). Erlkönige gehören zu den bestgehütetsten Geheimnissen in der Automobilindustrie. Mitunter sind die Hersteller selbst überrascht. Vor zwei Jahren standen von einer neuen Mercedes-S-Klasse schon vor ihrer offiziellen Präsentation Fotos im Internet. Die Aufnahmen erfolgten offenbar durch eine ferngesteuerte Drohne, die unbemerkt über dem Gelände schwebte. Bei Sicherheitsexperten sind die kleinen, wendigen und schnellen Flugmaschinen inzwischen berüchtigt. Sie können Arbeitsabläufe oder Lagerstellen ausspähen und mit ihren hochauflösenden Kameras durch Bürofenster vertrauliche Papiere oder Bildschirminhalte fotografieren. Sie können sich in interne Netzwerke einhacken, auf Dächern von Bürohäusern Hotspots absetzen und Zugangsdaten der internen WLANs übernehmen. Täter gewinnen die Kontrolle über ein Firmennetzwerk auch dadurch, dass sie in einem Computer eine sogenannte ‚Backdoor' installieren. Zu diesem Zweck müssen sie in das Gebäude einbrechen. Wie problemlos dies Sicherheitstestern gelang, ist im Internet nachzulesen. Es seien nicht alle Türen abgeschlossen oder durch Zugangskontrollsysteme verriegelt gewesen, heißt es unter anderem. Die Beispiele zeigen, dass Cyber-Kriminalität und physische Angriffe nicht so scharf voneinander zu trennen sind, wie es allgemein angenommen wird.

Häufig stößt man schon bei der Analyse des Ist-Zustands auf Verbesserungsbedarf

Neun von zehn Unternehmen waren in den Jahren 2020/2021 laut dem Digitalverband Bitcom Opfer digitaler und analoger Angriffe. Von ‚analog' spricht man, wenn Daten durch Innentäter oder Eindringlinge von Hand abgegriffen werden. Kapitalmarktorientierte Unternehmen müssen über solche Vorkommnisse öffentlich Bericht erstatten. „Was in die Presse gelangt, ist aber immer nur die Spitze des Eisbergs", sagt Michael Blaumoser, Geschäftsführer der Sicherheitsberatung SIUS Consulting GmbH. Wer nicht zur Publizität verpflichtet ist, schweigt in der Regel, um Kunden und Geldgeber nicht zu verunsichern. Die aber wollen inzwischen genau wissen, auf wen sie sich einlassen. „Früher hatte man nur einen Verlust, wenn ein Supplier ausgefallen ist. Jetzt besteht die Gefahr, dass der Ausfall eines Suppliers zur eigenen Insolvenz führt", so der Teilnehmer der Deloitte-Studie Lieferanten-Risikomanagement in der Automobilwirtschaft 2020. Lieferanten von OEMs müssen sich TISAX-zertifizieren lassen. Basis ist die ISO/IEC 27001, eine international anerkannte Norm für IT-Sicherheit und nicht-digitale Systeme wie Papier-Archive, Räumlichkeiten und Sicherheitskontrollen. „Zertifizierte Unternehmen fordern von ihren Auftragnehmern inzwischen ebenfalls entsprechende Nachweise. Es ist davon auszugehen, dass künftig auch Tier-2- und Tier-3-Lieferanten in die Pflicht genommen werden", so Christian Rentschler. Der IT-Experte ist Produktmanager bei Securiton Deutschland, einem führenden Spezialisten für gewerbliche und industrielle Sicherheitstechnik und Projektpartner im Forschungsprogramm des Bundes für die zivile Sicherheit. In diesem Programm arbeiten Behörden, Wissenschaft und Unternehmen an zukunftsweisenden Konzepten und Technologien zur Kriminalitäts- und Gefahrenabwehr, darunter das Bundeskriminalamt, das Fraunhofer IOSB, die Johannes-Gutenberg-Universität Frankfurt und die Fraport AG. Mit anderen Worten: Ohne Zertifizierung kein Geschäft! Allerdings haben es Sicherheitsarchitekturen auf den neuesten Stand zu bringen. Eine nicht geringe Anzahl hat sich mit dem Thema aber offenbar noch gar nicht auseinandergesetzt.

> **»Zertifizierte Unternehmen fordern von ihren Auftragnehmern entsprechende Nachweise. Es ist davon auszugehen, dass künftig alle Lieferanten in die Pflicht genommen werden.«**
>
> **Christian Rentschler,**
> Produktmanager bei Securiton

Es steige der Beratungsbedarf bei Unternehmen, die von Auftraggebern dazu angehalten würden, berichtet Experte Blaumoser. Häufig stoße man schon beim ersten Schritt, der Analyse des Ist-Zustands, auf erheblichen Verbesserungsbedarf. Dabei seien größere Unternehmen erkennbar nicht signifikant besser aufgestellt als kleinere. Potenzielle Täter gelangten allzu leicht und unbemerkt auf Firmengelände und bedrohlich nahe an Produktionen, Lager und Infrastruktureinrichtungen. Es reiche nicht selten ein ‚wichtiges Gesicht und ein Laptop unter dem Arm', um am Pförtner oder der Rezeption vorbeizukommen, weil keine Regelungen für sicherheitsrelevante Abläufe existierten. Viele Unternehmen verfügten beispielsweise über keine elektronische Zutrittsteuerung. Oder aber die installierten Sicherheitstechniken seien nicht aufeinander abgestimmt. Blaumoser: „Ein typischer Fehler ist es, einzelne Funktionen, etwa eine Einbruchmeldeanlage oder eine Videoanlage als separate Einrichtungen anzusehen. Dabei hat die Sicherheitstechnik in den letzten Jahren eine rasante Entwicklung genommen." Künstliche Intelligenz (KI) spielt dabei eine immer wichtigere Rolle.

Beispielsweise läuft in herkömmlichen Sicherheitsarchitekturen der Alarm einer Einbruchmeldeanlage an einer zentralen Stelle auf. Von dort aus wird versucht, auf den Bildschirmen der Videoüberwachung das Geschehen zu verifizieren. Anhand der Aufzeichnungen lassen sich die Tat rekonstruieren und Täter identifizieren. Moderne Videotechnik sorgt dagegen mit intelligenter Bildanalyse dafür, dass ein Schaden gar nicht erst entsteht. Rentschler: „Programmierte Algorithmen lösen bei kleinsten Auffälligkeiten, etwa im Verhalten von Personen, Alarmsignale aus, sodass frühzeitig Interventionsmaßnahmen ergriffen werden können."

Videotechnik lässt sich zudem mit mechanischen Schutzmaßnahmen vernetzen, etwa dem Perimeterschutz. Dies sind mit Detektionssensoren ausgerüstete Umzäunungen. Sobald einer der Sensoren anschlägt, nimmt das Kamerasystem mit moderner IPS-3D-Technologie automatisch die Verfolgung auf; es lässt den Angreifer oder Einbrecher nicht mehr ‚aus den Augen'. Die Meldungen der Sicherheitssysteme werden in einer Alarmzentrale erfasst und von dort aus wiederum weitere periphere Systeme wie Beleuchtungs- und Beschallungsanlagen ferngesteuert.

Hochfrequenztechnologie spannt einen Schutzschirm über das Firmengelände

Auch die neue Lieblingswaffe von Ausspähern und Angreifern, die Drohne, lässt sich mit intelligenter Technik abwehren. Hochfrequenz-Technologie spannt ähnlich einem militärischen Abwehrschirm gleichsam eine Schutzhülle über das Firmengelände. Nähert sich ein Flugobjekt, wird es anhand der vorhandenen – oder fehlenden – in der EU vorgeschriebenen digitalen Kennung (Remote ID) identifiziert. „Das System kann die Drohne gegebenenfalls schon vor ihrem Start erkennen und Interventionsmaßnahmen auslösen. Beispielsweise ist es möglich, die Kontrolle über die Drohne zu übernehmen", so Christian Rentschler von Securiton. Investitionen in mehr Sicherheit begegnen nicht nur irreparablen Imageschäden, Kundenverlusten, Regressforderungen oder hohen Strafzahlungen. Die Pandemie und Naturkatastrophen haben die Prämien in der industriellen Sachversicherung seit 2019 um gut 20 Prozent steigen lassen. „Dagegen stehen kostensenkende Maßnahmen wie Eigentragungsmodelle, höhere Selbstbeteiligungen und vor allem verbessertes technisches, organisatorisches und juristisches Risikomanagement", so die BDJ Versicherungsmakler GmbH. ■