Foto: ipopba - stock.adobe.com

Existenzgefährdend kann es für Sicherheitsdienstleister werden, wenn sie Opfer einer Cyberattacke sind. Ein entsprechender Versicherungsschutz sollte daher vorhanden sein.

Hoffentlich gut versichert

Wenn Sicherheitsdienstleister Opfer einer Cyberattacke werden und Kundendaten in die falschen Hände geraten - wie sieht es mit dem Versicherungsschutz aus?

BERND M. SCHÄFER

Vernetzte Systeme, auch von Sicherheitsdienstleistern, sind anfällig für Cyberattacken; diese benötigen daher einen besonderen Versicherungsschutz. Die Globalisierung, Inbegriff der Vernetzung, hat zur Verbreitung von Covid 19 über die ganze Welt maßgeblich beigetragen. Sicherheitsdienstleister stehen hier in einer besonderen Rolle: Denn einerseits sind sie ein Teil der Lösung, andererseits leiden sie unter den Bedrohungen wie andere Unternehmen auch.

Die Hafnium-Attacke

Am 3. März 2021 veröffentlichte Microsoft außerplanmäßig ein Sicherheitsupdate. Vier Sicherheitslücken ihrer Exchange-Server sollten damit geschlossen werden. Angreifer hatten sich über diese Lücken seit Dezember 2020 als Administratoren anmelden und Schadsoftware unbemerkt einschleusen können. Ab Februar 2021 wurden dann durch Massenscans Informationen von den betroffenen Systemen abgezogen. Stunden nach der Veröffentlichung des Sicherheitsupdates kam es zum großflächigen Angriff auf die infizierten Exchange-Server.

Sicherheitsunternehmen bieten grundsätzlich die gleichen Angriffsflächen wie alle anderen Unternehmen in Deutschland. Es drohen Verluste von Kundendaten, des Rechnungswesens und der Personalverwaltung. Daraus kann ein Stillstand des Unternehmens resultieren und ein Betriebsunterbrechungsschaden. Dieser ist über eine Cyberversicherung versicherbar. Bei Sicherheitsdienstleistern gibt es jedoch noch eine weitere Problematik. Hier geht es nicht nur um irgendwelche Kundendaten, sondern um die Daten inklusive Foto- und Videomaterial der zu schützenden Objekte, die auf den Servern einer NSL lagern. Dies hat eine andere Qualität, da sich dadurch Tore für weitergehende Angriffe öffnen. Zudem muss sehr zeitnah gehandelt werden, da die Angreifer die Bilder der Objekte weiterverkaufen können, wodurch beispielsweise die Positionen von Überwachungskameras preisgegeben werden.

Bei drei Kunden von Atlas war der Angriff erfolgreich. In zwei dieser Fälle bestand eine Cyberversicherung. Die sofort eingebundenen Krisendienstleister machten die Unternehmen wieder sicher und betriebsbereit. Datenabflüsse gab es nicht. Gleichwohl zeigt dies die besondere Brisanz der in der Sicherheitswirtschaft digital verfügbaren Daten von Schutzobjekten auf. Werden sicherheitssensible Daten abgezogen, sind die Folgen unübersehbar.

Versicherungsschutz gegen Cyberangriffe

Es stellt sich auch die Frage, ob das Sicherheitsunternehmen für Schäden bei Auftraggebern haften könnte, wenn sich herausstellt,

dass sensible Kundendaten abgeflossen sind. Denkbar sind hier zum Beispiel Schäden durch erfolgreiche IT-Einbrüche, bei denen die Sicherheitsarchitektur des Auftraggebers auf Basis der entwendeten Daten mit Insiderkenntnissen ausgehebelt wurde. Die Haftung wird im Einzelfall bewertet werden müssen. Allerdings kann zum Beispiel das bewusste Nichtaufspielen von Hersteller-Updates ein schuldhaftes und damit haftungsbegründendes Verhalten darstellen. Der entsprechende Cyberhaftpflicht-Versicherungsschutz des Unternehmens muss darauf abgestimmt sein, um sich gegen Schadenersatzansprüche verteidigen zu können und eventuelle Ersatzleistungen vom Versicherer tragen zu lassen. Zu berücksichtigen sind auch andere mögliche Folgen. Abgesehen von der Haftung, dürfte es einen sehr großen Reputationsschaden für das Sicherheitsunternehmen geben. Die Kosten für geeignete PR-Maßnahmen sind Teil der Cyberversicherungsleistungen.

Wertvolle Unterstützung

Kommt es bei einem Sicherheitsdienstleister zu dem Abfluss von personenbezogenen Daten, so wird es sich regelmäßig um einen anzeigepflichtigen Vorfall nach dem Bundesdatenschutzgesetz (BDSG) handeln. In einem solchen Fall müssen alle betroffenen Personen nach § 66 BDSG benachrichtigt werden. Dies wird in den meisten Fällen die Unternehmen überfordern, denn das rechtssichere, standardisierte und nachweisbare Abtelefonieren möglicherweise tausender Kunden übersteigt die vorhandenen Kapazitäten. Die gesetzlich mögliche, öffentliche Bekanntmachung nach § 66 (3) Nr. 3 BDSG käme allerdings einem Todesurteil gleich. Alternativ wäre die Beauftragung eines Callcenters, weil dort für derartige Aufgaben Kapazität und Know-how vorhanden sind. Auch dies ist ein Teil des Leistungspakets der Cyberversicherung.

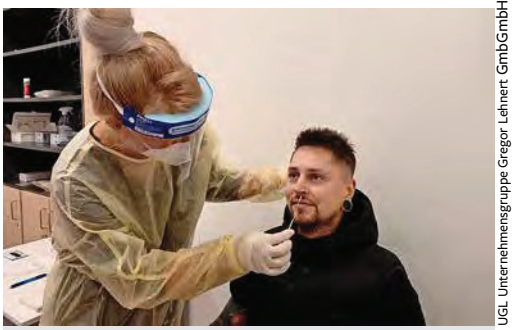
Verstöße gegen Datenschutzbestimmungen können zu Strafverfahren nach § 42 BDSG führen. Ein besonderes Thema für die Träger der Gewerbeerlaubnis für Bewachungsunternehmen ist der drohende Entzug wegen fehlender Zuverlässigkeit nach § 34a (1) Nr. 4 Gewerbeordnung, wozu die Verurteilung zu einer Freiheitsstrafe oder einer Geldstrafe von mindestens 90 Tagessätzen führen würde. Der Fortbestand des Unternehmens wäre gefährdet. Bei der Verteidigung gegen diese Vorwürfe geht es um mehr als nur um eine Geldstrafe. Die Strafrechtsschutzversicherung ist hier das geeignete Instrument, um die Kosten für die Verteidigung im Strafverfahren loszuwerden. ■

Atlas Versicherungsmakler für Sicherheits- und Wertdienste GmbH, www.atlas-vsw.de

„Werden sicherheitssensible Daten von Schutzobjekten abgezogen, sind die Folgen unübersehbar.“

Bernd M. Schäfer, Geschäftsführender Gesellschafter der Atlas Versicherungsmakler für Sicherheits- und Wertdienste GmbH

Foto: Atlas Versicherungsmakler für Sicherheits- und Wertdienste GmbH



UGL Unternehmensgruppe Gregor Lehnert GmbGmbH

Versicherungs für neue Aufgaben

Die Flexibilität der Sicherheitsunternehmen hat im vergangenen Jahr zu deutlichen Umsatzzuwächsen geführt. Ging es zu Beginn der Pandemie um Zutrittskontrollen in Supermärkten und Krankenhäusern, so wandelten sich die Anforderungen hin zum Patientenmanagement oder zum Testen von Mitarbeitern. Selbst das Betreiben von kompletten Impfzentren – inklusive des ärztlichen Dienstes darin – wird von Auftraggebern angefragt.

Wichtig ist, dass die Betriebshaftpflichtversicherung des Dienstleisters flexibel gestaltet ist. Eine marktübliche Betriebsbeschreibung, die ein „Bewachungsunternehmen nebst branchenüblichen Nebentätigkeiten“ versichert, genügt nicht. Da es nicht möglich ist, diese Tätigkeiten im Vorhinein exakt zu definieren, muss die Betriebsbeschreibung umfassend formuliert sein, damit das Unternehmen flexibel agieren kann. Gleichzeitig muss ein klarer Trennstrich zu allen ärztlichen Leistungen gezogen werden, denn diese können nur über eine separate Arzthaftpflichtversicherung abgedeckt sein.

Auch skurrile Dienstleistungen werden angefragt. So sollte ein Sicherheitsdienstleister, der den Pfortendienst in einem großen produzierenden Unternehmen versieht, die von den Mitarbeitern zuhause durchgeführten Schnelltests bei der Einlasskontrolle auf das Ergebnis hin prüfen und abstempeln. Die Mitarbeiterin weigerte sich, denn aufgrund der Fehlerquoten sei es denkbar, dass ihr ein falsch negativ ausgewiesener Test vorgelegt würde und sie sich damit infizieren könnte. Abgesehen von der arbeitsrechtlichen Problematik (Verlegung von Arbeitszeit (Testen) in die Freizeit des Arbeitnehmers) ein sicherlich beachtliches Argument. Es zeigt aber, dass es immer weiter geht mit den Anforderungen an die flexible Sicherheitswirtschaft - und den notwendige Versicherungsschutz.