Unsichtbare Grenzen überwinden

Von Holger Köster

Holger Köster
Vorsitzender des BDSW Arbeitskreises Wirtschaftsschutz

Wir sprechen gerne von einer ganzheitlichen Sicherheit. Also einem Maß an Sicherheit, das im Stande ist, gängige Angriffe abzuwehren. Doch in der Praxis bleibt das allzu oft ein unerreichter Idealzustand. Einer der Gründe dafür ist eine unsichtbare Grenze, die immer noch zwischen IT- und physischer Sicherheit gezogen wird.

Die einzige Gemeinsamkeit der beiden Schutzbereiche ist oft, dass sie unter dem Dach eines gemeinsamen Unternehmens aktiv sind. Damit erschöpfen sich aber häufig auch schon die Schnittstellen. In nicht wenigen Unternehmen gelten Cyber- und physische Sicherheit als völlig unterschiedliche Welten. Oft ist zu hören, dass es an gegenseitigem Verständnis fehle.

Dabei sind die Gemeinsamkeiten wesentlich prägnanter als das Trennende. Das Ziel, mehr Sicherheit zu schaffen, ist identisch, mögen auch Arbeitspraxis und Herangehensweise unterschiedlich sein. Beides ist wichtig und darf nicht zulasten des anderen priorisiert werden. Wo es zwei Einfallstore gibt, müssen beide gesichert werden. Und vor allem ist das eine ohne das andere nicht denkbar. IT-Schutz 2.0 ist nur dann etwas wert, wenn der physische Schutz zumindest gleichrangig ist. Und umgekehrt.

Deshalb unsere Empfehlung: IT- und physische Sicherheit sollten sich deshalb nicht isoliert voneinander organisieren. Vielmehr wäre es sinnvoll, wenn diese wichtigen Teilkomponenten der Unternehmenssicherheit zusammenrücken und miteinander vernetzt werden.

In diesem Sinne: Bleiben Sie auf der sicheren Seite!

Bild: Alexander Dreher / Pixelio.de

Die beste IT-Sicherheit nützt nichts, wenn der physische Schutz lückenhaft ist.

IT-Schutz und physische Sicherheit: Weshalb das eine ohne das andere Stückwerk bleibt

Von Klaus Henning Glitza

Jeder dürfte ihn wohl kennen, den Vergleich eines Unternehmens mit einer Burg. Und die daraus gezogene Lehre, dass es nichts nützt, die oberirdischen Mauern und Zinnen zu bewachen, wenn sich Angreifer aus dem Untergrund ins Innere graben können. Konkret gemeint ist damit, dass die Abwehr von IT-Attacken als Angriffsszenarien der Neuzeit mit konventionellen physischen Schutzmaßnahmen Schritt halten muss.

Klaus Henning Glitza

Ehemaliger Redakteur der Hannoverschen Allgemeinen Zeitung, Träger des Deutschen Förderpreises Kriminalprävention (Stiftung Kriminalprävention, Münster) und seit 2003 als Fachjournalist für Sicherheitsfragen tätig.

Das hat zweifelsohne gewirkt, aber auch zu einem Paradoxon geführt. Während sich die IT-Sicherheit in vielen Bereichen verbessert hat, wenn auch nicht in dem Maße, die den ITlern vorschwebt, ist der umfassende physische Schutz nicht adäquat vorangekommen. Oftmals stehen die Schutzansätze sogar in Konkurrenz zueinander. Firmenchefs sprechen offen davon, dass beides nicht gleichermaßen finanzierbar sei. Oder sie vertreten die Ansicht, dass mit der IT-Sicherheit den Hauptrisiken für ihr Unternehmen entgegengetreten werde. Alles andere sei auch schlimm, aber nicht im Entferntesten so unternehmenskritisch. Eine gefährliche Fehleinschätzung.

Denn – eigentlich eine Binsenwahrheit – ein partieller Schutz kann nur zu einer partiellen Sicherheit führen. Wer glaubt, mit physischen Schutzmaßnahmen (in grober Zusammenfassung: Perimeterschutz, Zutrittskontrolle, Zugangsbeschränkung und Überwachung kritischer Bereiche) würden überwiegend Einbrecher und Diebe abgehalten, liegt gründlich falsch. Es ist eine, in Hollywoodstreifen oft und gerne in Szene gesetzte Illusion, dass Angreifer nur ein paar Mal hastig auf Tasten drücken müssen, um in fremde IT-Systeme einzudringen. Die wahre Welt sieht anders aus.

Und das nicht nur, weil es kaum möglich ist, im Handumdrehen andere PCs und Server zu entern, sondern weil die Dunkelmänner aller Sorten längst auf die erhöhte IT-Sicherheit reagiert haben. Und das nicht mit raffinierteren Hackingmethoden, sondern mit einer Rückbesinnung auf die Werkzeuge von gestern. Nach der Devise: Mögen Schließanlagen noch so raffinierten Aufsperrtools widerstehen, gegen die seit Menschengedenken gebräuchliche Axt sind sie oft machtlos.

Schwachstellen sind Angreifers Darling. Ob Ansatzpunkte für Attacken im physischen oder IT-Bereich liegen, ist den Dunkelmännern relativ egal. „Auf das Ergebnis kommt es an", dieser alte Spruch gilt hier in besonderer Weise.

Es ist ein offenes Geheimnis, dass in vielen Unternehmen die Cybersicherheit oder physische Sicherheit befassten Personen nur selten kooperieren. In einigen Fällen können oder wollen sie noch nicht einmal miteinander. Eifersüchteleien und der Dünkel der angeblichen technologischen Überlegenheit tun das ihrige. In größeren Unternehmen berichten die handelnden Personen der beiden Bereiche häufig unterschiedlichen Führungskräften. Der eine an den CEO, der andere eine Stufe darunter. Das Ergebnis: Nichts fließt wirklich zusammen. Jeder macht sein Ding in der aus Eigensicht optimalsten Weise. Doch es bleibt bei Einzelergebnissen, die nicht auf einen Nenner kommen.

Noch gravierender wirkt sich aus, wenn IT- oder physische Sicherheit fremdvergeben werden. Jeder Auftragnehmer trachtet dann häufig in nachvollziehbarer Weise danach, das für sein Teilgebiet beste Ergebnis abzuliefern. Ob das mit dem Aspekt der wünschenswerten ganzheitlichen Sicherheit zusammenpasst, ist eine zweite Frage – und oftmals auch gar nicht das Auftragsziel.

Ein zurückliegender Fall macht deutlich, dass sich Cyber- und physische Sicherheit gegenseitig bedingen. Bei Tiefbauarbeiten wurde auf dem Betriebsgelände eines niedersächsischen Unternehmens ein vergrabener Router entdeckt. Mit diesem war es möglich, von außen gesteuert auf das betriebliche Netzwerk zuzugreifen. Nach Erkenntnissen des niedersächsischen Verfassungsschutzes gab es für dieses sinnbildliche „trojanische Pferd" keinerlei Schutz.

Der beispielhafte Fall belegt: Die IT-Sicherheit kann noch so gut und ausgereift sein, sie wird dennoch zur Makulatur, wenn in anderen Bereichen meterbreite Lücken klaffen. Lücken, die

selbstredend umgehend genutzt werden, denn die Angreifer sind bekanntermaßen alles andere als dumm.

Weitere reale Beispiele mögen das belegen. So fand sich im Besucherraum eines Unternehmens ein offen an der Wand angebrachter Router. Lange Zeit hatte niemand Notiz davon genommen. Das Teil war ordentlich angebracht und alle glaubten, es werde wohl schon seine Richtigkeit haben. Die Tarnung liegt im Alltäglichen, heißt es nicht umsonst. Erst ein Sicherheitsexperte, der aufgrund eines anderen Vorfalls eingeschaltet wurde, kam dem trojanischen Router auf die Spur. In einem anderen Unternehmen wurden sensible IT-Leitungen durch öffentlich zugängliche Räume geführt. Es dauerte nicht lange, bis Angreifer diesen Schwachpunkt entdeckten. Professionell wirkende „Handwerker" erschienen, um vor den Augen aller Besucher die Leitungen anzuzapfen. Niemand dachte sich etwas dabei. Handwerker im Einsatz, das ist schließlich etwas ganz Normales. So flossen über längere Zeit sensible Informationen ungehindert ab. Erst als sich Verdachtsmomente ergaben, kam die Attacke ans Licht.

„Handwerker" traten auch in einem weiteren Fall in Erscheinung. Dabei nutzten die Täter Insiderwissen. Sie wussten aus belauschten Mitarbeitergesprächen, dass die betriebsinternen IT-Geräte einmal im Jahr inspiziert wurden. Der Mann an der Pforte schöpfte deshalb keinen Verdacht, als „Servicekräfte" erschienen, und ließ sie rein. Erst als Wochen später die echten Handwerker auftauchten, flog die Legende auf. Doch bis dahin war es bereits zu einem massiven Abfluss kritischer Daten gekommen.

Eine kleine Nachlässigkeit und schon ist das IT-System von einem Virus oder Wurm befallen.

Bild: Antje Delater / pixelio.de

Genauere Details sind nicht bekanntgegeben worden. Es liegt aber nahe, dass Keylogger installiert worden sind. Dabei handelt sich um kleine Aufzeichnungsgeräte, die sämtliche Eingaben des PC-Nutzers protokollieren. Darunter natürlich auch Kenn- und Passwörter. Gesteckt werden diese Logger meist in den unteren Slot, der zur Tastatur führt. Das dauert nur Sekunden. Über eine integrierte Steckverbindung bleibt der Kontakt zur Tastatur erhalten. Es gibt diese Keylogger auch als Softwareversionen oder als Modelle, die die Protokolldaten über Funk oder Netzwerke versenden. Es bedarf deshalb nach der Installation nicht zwingend eines Zugangs zum „heißen Raum".

Kennzeichnend für diesem Fall: Einige Mitarbeiterinnen und Mitarbeiter wunderten sich zwar über das Vorgehen der „Handwerker", das sich vom üblichen Arbeitsverhalten der regulären Kräfte unterschied. Doch niemand traute sich, Vorgesetzte oder Sicherheitsverantwortliche zu informieren. Man wollte nicht als „Oberverdachtsschöpfer" dastehen oder als jemand, der Entscheidungen „von oben" infrage stellt.

Eine Angriffsoption liegt auch in gefakten Einbrüchen. Das heißt: Die Täter brechen nicht ein, um die typischen materiellen Werte zu erbeuten, sondern, um gezielt Informationen zu stehlen oder deren Diebstahl vorzubereiten. Dabei sind die Täter nicht immer so dumm, dass ihre tatsächlichen Ziele augenscheinlich werden, wie es in zwei Fällen geschah. Beim Fall Nummer 1 drangen die Täter ausschließlich in ein Obergeschoss ein, in dem sich die Server befanden, und ließen die anderen, besser erreichbaren Etagen außen vor. In zweiten Fall vergruben die Kriminellen die zum Schein mitgenommene Beute so nachlässig, dass sie von einem Forstmitarbeiter gefunden wurde. Das legte letzten Endes die wahren Ziele der Ganoven offen. Doch das sind Ausnahmen. Selbst erfahrene Kriminalisten kommen nicht umhin, bestimmte Einbrüche trotz eines „Geschmäckles" der allgemeinen Kriminalität zuzuordnen.

Und immer noch funktioniert der uralte Trick, dass hochwertige USB-Sticks in der Nähe von Unternehmen oder

Bild: Tim Reckmann / pixelio.de

Will er materielle Beute machen – oder geht es eher um Datendiebstahl? Mancher Einbruch hat andere Hintergründe als auf den ersten Blick vermutet.

auf deren Parkplätzen „verloren" werden. In der Hoffnung, dass diese Speichermedien von Mitarbeitern gefunden werden, die sie dann nicht etwa zum Fundbüro bringen, sondern im Betrieb einsetzen. Und schon ist eine Spyware oder ein anderes Schadprogramm im System.

Es ist unbestreitbar, dass alle diese Fälle im Versuch steckengeblieben wären, hätte es eine umfassende physische Sicherheit und nicht zuletzt auch Sensibilität gegenüber solchen Angriffsmöglichkeiten gegeben. Der Fall mit den falschen Handwerkern, Stichwort Keylogger, zeigt auf, dass es fatal ist, wenn Verdachtsmeldungen unterlassen wurden. In diesem Punkt sind Unternehmen gut beraten, wenn sie zu solchen Meldungen ermuntern. Und die Parole ausgeben: Lieber einmal zu viel melden als einmal zu wenig. Die Mitarbeiter müssen wissen, dass ihnen eine Meldung nicht zum Nachteil gereicht.

Eine zweite Lehre aus den vorstehenden Zeilen: IT- und physischer Schutz sollten enger zusammenrücken, im Idealfall sogar in einer Hand liegen. Die Zeiten, in denen jeder auf seine Art vor sich „hin muckelte" sind endgültig vorbei. Da sich die Bedrohungslage weltweit verschärft hat und auch kriminelle Strukturen im Vormarsch sind, können alte Rezepte nur noch bedingt helfen. Es muss auf Neustart geschaltet werden.

Eine gute Lösung wäre es, die künstliche Grenze zwischen IT- und physischer Sicherheit zu überwinden. Ein erster Schritt dazu könnte sein, dass diese beiden Bereiche regelmäßig miteinander konferieren, um

sich fachlich auszutauschen und Synergien zu identifizieren. In der Folge wäre eine gemeinsame Leitung zu überlegen. Nach dem Modell des Chief Information Security Officer (CISO), der für die gesamte IT-Sicherheit zuständig ist, könnte ein Fachmann beide Aufgabenbereiche bündeln und zusammenführen. Das setzt natürlich voraus, dass diese Kraft in beiden Teilbereichen fachkundig ist und sie als gleichermaßen wichtige Komponenten zu würdigen weiß. Ist die Sicherheit ganz oder teilweise outgesourct, sind Wach- und Sicherheitsdienste die richtigen Ansprechpartner. Gut aufgestellt, beherrschen sie selbst oder in Kooperation mit Partnern beide Schutzbereiche.

Wie auch immer: Für die Sicherheit von Unternehmen wäre es auf jeden Fall ein beträchtlicher Gewinn, wenn zusammenkommt, was schon lange zusammengehört.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

Informationsblätter zum Wirtschaftsschutz

Unternehmen besitzen Know-how, an denen außenstehende Dritte interessiert sind. Vielfach sind auch Innentäter ein erhebliches Risikopotenzial für den Abfluss von Know-how. Die neuen Informationsblätter „Bedrohung durch Innentäter“ und „Pre-Employment-Screening“ bieten Hilfestellungen, um die mit Personal verbundenen möglichen Sicherheitsrisiken zu reduzieren.
www.verfassungsschutz.de

Bitkom-Umfrage: Cyberkriminalität

Nach dieser Befragung waren 75 Prozent der Internetnutzer 2022 von Cyberkriminalität betroffen. 46 Prozent der Befragten berichteten, dass persönliche Daten ungefragt weitergegeben wurden. Bei 27 Prozent wurde der Computer mit Schadprogrammen infiziert. Nur 22 Prozent hatten keine Erfahrungen damit gemacht. Nur ein Fünftel der Opfer wendete sich an die Polizei.
www.bitkom.org

G DATA Cyberdefence-Studie: Cybersicherheit in Zahlen

Ein Drittel der Angestellten gefährdet die IT-Sicherheit in deutschen Unternehmen. Mehr als ein Drittel der Befragten beurteilt die persönliche Kompetenz in Sachen IT-Sicherheit als gering oder sehr gering. Das höchste Wissen im Bereich IT-Sicherheit haben Belegschaften der Branchen Telekommunikation und Informationsdienstleistungen.
www.data.de

PwC Corporate Security Survey

Laut dieser Studie aus 2022 hat sich die Unternehmensfunktion der Corporate Security (Unternehmenssicherheit) in den letzten Jahren grundlegend gewandelt. Im Fokus stehen die Bewältigung von Risiken durch Kriminalität, Cyberangriffe, Spionage, Vandalismus oder geopolitische Ereignisse. 80 Prozent der Befragten stuft die Unternehmenssicherheit als geschäftsförderndes Element ein.
www.pwc.de

RA Dr. Berthold Stoppelkamp
zuständiges Geschäftsführungsmitglied für den BDSW Arbeitskreis Wirtschaftsschutz