Aus der digitalen Welt gekickt

Von Holger Köster

Holger Köster

Vorsitzender des BDSW-Arbeitskreises Wirtschaftsschutz

Es gehört zum Grundwissen jedes Sicherheitsexperten, dass es eine hundertprozentige Sicherheit nicht gibt. Das gilt nicht zuletzt für die IT-Infrastruktur, auf deren Funktionieren jedes Unternehmen unverzichtbar angewiesen ist. Fallen die Systeme aus, folgt ein IT-Blackout.

Dennoch ist die IT trotz ihrer immensen Bedeutung in einer zunehmend digitaler werdenden Welt oftmals ein Stiefkind. Mit PCs und Servern, so erscheint es jedenfalls in verkürzter Weise rein betriebswirtschaftlich Rechnenden, ist unmittelbar kein Geld zu verdienen. Dass dem nicht so ist, wird oftmals erst in aller Deutlichkeit klar, wenn die Systeme nicht mehr zu Verfügung stehen.

Selbst abgeklärte Fachleute sind oft überrascht, was alles zum Erliegen kommt, wenn wir auf einen Schlag aus der digitalen Welt gekickt werden. Die unerlässlichen digitalen Kundenkontakte und jede andere Art von Kommunikation (auch die Festnetztelefonie, die schon lange über die Digitalnetze läuft), Akquisitionen, Finanzbuchhaltung, Lohnbuchhaltung, laufende Projekte – alles fällt auf den Nullpegel zurück.

Deshalb ist es unerlässlich, der IT-Sicherheit erhöhte Aufmerksamkeit zu widmen. Dass es eine hundertprozentige Sicherheit nirgendwo gibt, darf kein Grund sein, den Kopf in den Sand zu stecken und aufzuhören, ein rundum angemessenes Maß an Sicherheit anzustreben. Nur

Datenschutz ist richtig und wichtig. Doch um folgenschwere IT-Angriffe abzuwehren, bedarf es weitaus mehr.

eine umfassende und vor allem allseits gleichmäßig hohe Sicherheit schützt davor, allzu leicht Opfer zu werden. Denn wer solide Sicherheit etabliert, wehrt bereits einen Großteil der Angreifer ab, die größeren Aufwand scheuen oder schlichtweg mit schwer zu „knackenden" IT-Systemen fachlich überfordert sind. Man sichert ja auch nicht die Haustür alleine, wenn sich die Hintertür einfach aufhebeln lässt …

Allen, die von ihren Mitarbeitenden Sensibilität und Achtsamkeit fordern, sei in Erinnerung gerufen, dass diese kaum motiviert werden können, wenn auf der Unternehmensseite deutliche Sicherheitslücken klaffen.

In diesem Sinne: Bleiben Sie auf der sicheren Seite.

Gegen die Begehungsarten moderner IT-Krimineller nehmen sich Spams schon fast harmlos aus. Ganz ohne sind sie dennoch nicht. Schon beim Öffnen von Spamnachrichten kann ein Trojaner die IT-Systeme infizieren.

Vernetzt mit einem globalen IT-Umfeld, das keinesfalls voller Gutmenschen ist

Von Klaus Henning Glitza

Sich abzusichern und sich gegen bekannte Risiken zu schützen ist gut und richtig, doch ein perfekter Schutz kann damit nicht eingekauft werden. Das gilt in besonderen Maße für IT-Infrastrukturen, die uns mit einer Welt vernetzen, die keinesfalls voller Gutmenschen ist.

Unternehmen stehen bekanntermaßen im Fokus von kriminellen, möglicherweise fremdstaatlich gelenkten Angreifern. Ihre Führungskräfte sollten sich deshalb niemals in Sicherheit wiegen, sondern intensiv überlegen, was im Vorfeld getan werden kann – und auch, was zu tun ist, wenn das sprichwörtliche Kind erst einmal in den Brunnen gefallen ist.

Jeder kennt den etwas verkürzt wiedergegebenen Ausspruch „Houston, wir haben ein Problem!". Doch nicht alle erinnern sich daran, was geschah, nachdem die Besatzung von Apollo 13 im April 1970 diesen Funkspruch absetzte. Die maßgeblichen Mitarbeiter des Lyndon B. Johnson Space Centers drehten sich um und steuerten endlose Regalwände an. Was irritierend wirkte, hatte seinen klaren Sinn. Sie suchten in Aktenordnern nach einer Lösung, einen Plan B für das Apollo-Problem – einem explodierten Sauerstofftank. In den Aktenordnern waren alle denkbaren Szenarien hinterlegt. Hand aufs Herz: Haben Sie auch diese Möglichkeit, wenn die Echtlage, ein IT-Angriff, zum Tragen kommt?

Vorbereitet sein auf den Fall der Fälle, das ist das A und O. Selbst Organisationen mit ausgereiften Sicherheitsprogrammen und -strukturen können sich vor Angreifern, die jeden Tag ein bisschen besser werden, nicht sicher sein. Doch es gibt Früherkennungsindikatoren.

Denn IT-Angriffe kommen nicht aus dem Nichts, sie haben eine detektierbare Vorgeschichte. Marc Becker, Managing Director der Palladium GmbH, die als Ransomware-Readiness- und Digital-Risk-Protection-Service-Provider mit realen Fällen befasst ist, berichtet, wie Attacken arbeitsteilig abgewickelt werden können. Oft sind es nicht die Angreifer selbst, sondern andere sogenannte Threat Actors, die sich den Erstzugang in das IT-Netzwerk des späteren Opfers verschaffen. Die damit zusammenhängenden Daten werden über das Darknet, Foren oder Messagingdienste an „Interessierte", in der Regel organisierte Täterstrukturen, verkauft. Das heißt, der bevorstehende Angriff verläuft vielmals keinesfalls spurenlos. Erkennbar sind solche Warnzeichen durchaus – jedoch nur für diejenigen, die Dark-Web-Foren und Börsen mittels sorgsam gepflegter Undercover-Konten professionell überwachen und analysieren. Doch welche, nicht selten unterbesetzte IT-Abteilung kann das neben dem anspruchsvollen Tagesgeschäft schon stemmen?

Zudem verlaufen Penetrationen des Netzwerkes und die letztliche Attacke selten parallel. Im Regelfall sind die IT-Systeme bereits einige Zeit kompromittiert, bevor die Täter zum Finale ansetzen. Oft vergehen je nach Angriffsart Wochen oder mehrere Monate, bis die Threat Actors offen in Erscheinung treten.

Denken wir daran: Jede Art von Konflikten der Neuzeit geht mit IT-Attacken einher. Der Krieg zwischen der Ukraine und der Russischen Föderation ist auch ein Krieg der Hacker, wobei Waffengleichheit zu herrschen scheint. Auch zwischen den USA und Rotchina tobt ein erbitterter Kampf der Cyberarmeen. Neuerliche Attacken haben ehemalige Sowjetrepubliken wie Georgien getroffen. Und auch Deutschland ist längst im Fokus. In einigen Fällen ließen sich die Attacken bis nach Russland zurückverfolgen. Sie haben nach Kreml-Lesart „natürlich" nichts mit der Moskauer Regierung oder deren nachrichtendienstlichen Erfüllungsgehilfen zu tun. Natürlich …

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

Der Geldkoffer zur Übergabe des Lösegeldes hat im Zeitalter der Ransomware-Attacken ausgedient. Die Cyberkriminellen verlangen, dass die geforderten Erpressungssummen digital, also per Kryptowährung à la Bitcoin, gezahlt werden. Das erschwert es, die Spur des Geldes zu verfolgen, macht es aber nicht unmöglich.

Bild: Thommy Weiss/pixelio.de

Die Verfassungsschutzbehörden wissen es allerdings besser. „Im Zuge des russischen Angriffskrieges in der Ukraine konnten Überschneidungen zwischen nachrichtendienstlichen Akteuren und solchen aus dem Bereich Ransomware festgestellt werden“, teilt Dr. Florian Volm vom Bayerischen Landesamt für Verfassungsschutz mit. Verschiedene, ursprünglich rein wirtschaftlich motivierte Cybercrimegruppierungen hätten sich „mit einer der beiden Kriegsparteien solidarisiert und führten Angriffe auf den jeweiligen Gegner durch oder hätten solche angedroht, um den Gegner zu schwächen beziehungsweise die Position der eigenen Seite zu stärken“. Dazu zählen laut Dr. Volm auch Gruppierungen, die im Zusammenhang mit Ransomware-Angriffen bekannt sind. Darüber hinaus kam es zu Angriffen mit sogenannten Wipern auf ukrainische Ziele. Bei Wipern (englisch to wipe = unbrauchbar machen) handelt es sich um Schadprogramme, die Dateien auf einem System mit einem bestimmten Wert überschreiben und somit irreversibel zerstören. „Diese Schadprogramme tarnten sich auf den ersten Blick als Ransomware, um das Opfer zu verwirren und möglicherweise zu falschen Gegenmaßnahmen zu verleiten. Diese Wiper wurden eher wahrscheinlich durch staatliche oder staatlich gesteuerte Akteure zu Sabotagezwecken eingesetzt“, erläutert der Verfassungsschutzexperte.

Die Stoßrichtungen von Angriffen sind breit gefächert. Sie reichen von Erpressungen, nachdem die IT-Infrastruktur verschlüsselt wurde, den sogenannten Ransomware-Attacken, über das gezielte Löschen von Daten bis hin zur Veröffentlichung von zuvor exfiltrierten sensiblen Daten der gehackten Unternehmen.

Bei Ransomware-Angriffen bewegen sich Angreifer meist schon lange im Voraus im Zielnetz, bevor es zu Lösegeldforderungen kommt. Es ist aus Expertensicht durchaus üblich, dass sich die Täter erst einmal im Netzwerk „umsehen“, um möglichst viele Ansatzpunkte für die spätere Verschlüsselung von Unternehmensdaten zu gewinnen. Selbst im Zuge eines Angriffs können immer noch Folgeschritte erfolgen, um den Druck auf das Opferunternehmen zu erhöhen beziehungsweise Nachschlag zu den ursprünglichen Forderungen zu erhalten.

Eine weit verbreitete Vorbereitungstat ist es, Konten der Mitarbeiter durch gezieltes Ausspähen der Zugangsdaten (Phishing Angriffe) zu übernehmen. Je nach Zielsetzung der Kriminellen können dann über gekaperte E-Mail-Accounts anstößige und/oder geschäftsschädigende Texte verschickt werden oder die Zugänge werden zur Einbringung von Schadsoftware an den Kontrollinstanzen der Firma vorbei verwendet.

Deshalb sei es in Fall X von enormer Bedeutung zu klären, mit wem man es eigentlich zu tun hat, macht der IT-Sicherheitsprofi und frühere Chief Security Adviser von Microsoft, Sebastian Rohr, deutlich. Sind es Profis, die mit allen Wassern gewaschen sind, oder Trittbrettfahrer, die Professionalität nur vortäuschen? Um das in Erfahrung zu bringen, seien Verhandlungen mit den Angreifern unverzichtbar, rät Rohr. Doch solche Gespräche müssen von Profis geführt werden, die das Metier und ihre hochkriminellen Akteure kennen.

Sich ein Schadprogramm einzufangen, das geht heute so schnell wie nie zuvor. Die Methoden der Angreifer sind zunehmend raffinierter geworden. Musste früher der Anhang einer Mail angeklickt werden, um sich einen toxischen Code einzuhandeln, genügt aktuell bereits das bloße Öffnen einer Mail. In der E-Post oder auf Webseiten können beispielsweise winzige unsichtbare Pixel versteckt sein, die das Nachladen weiterer Schadprogramme ermöglichen. Ebenso riskant ist das Aufrufen der in Mail angegebenen Webseiten, die entweder gehackt oder gefälscht sind und bereits beim Besuch Trojaner aktivieren. Aber beim ganz normalen Surfen können IT-Nutzer auf toxische Seiten geraten, die nicht von Virenscannern erkannt werden.

IT-Sicherheitsexperten wie Sebastian Rohr und Marc Becker gehen davon aus, dass viele IT-Netzwerke bereits mit einem Schadprogramm infiziert sind, ohne dass die Nutzer auch nur das Geringste davon

Geld sparen bei der IT-Sicherheit: ein zweifelhafter Weg in Zeiten, in denen die Gefährdungspotenziale überproportional wachsen und sich niemand sicher fühlen kann.

Bild: Jorma Bork/pixelio.de

ahnen. Dies dürfte insbesondere dann der Fall sein, wenn es den Angreifern um das Abgreifen von Daten geht. Ein weiteres Szenario könnte sein, dass die Voraussetzungen für einen späteren Angriff geschaffen werden, der zu einem strategisch oder taktisch sinnvollen Zeitpunkt realisiert werden soll.

Zweifellos: Die Gefahren sind überproportional gewachsen, aber ist es die IT-Sicherheit auch? Ein ausländischer IT-Sicherheitsexperte hat jüngst beklagt, dass die sicherlich wichtige IT-Compliance einen weitaus höheren Stellenwert genießt als der Schutz vor Angriffen. Doch beides ist mindestens gleichrangig.

Obwohl die Schäden durch Ausfall der IT-Systeme unermesslich sind und bis zur Geschäftsaufgabe reichen können, ist namentlich im Mittelstand die Sorglosigkeit groß. Dabei gibt es ein aktuelles Beispiel, das zu denken geben sollte. Ein Küchenmöbelhersteller musste nach einem IT-Angriff Insolvenz anmelden.

Die Ignoranz gegenüber den IT-Risiken ist teilweise der Tatsache geschuldet, dass nicht wenige Chefs der älteren Generationen angehören und mit der IT nicht übermäßig viel am Hut haben. Daneben sind die Führungskräfte oftmals weitreichend durch das Tagesgeschäft gefordert bis überbeansprucht. Hinzu kommt, dass es oft an professionellem IT-Personal fehlt. Hier muss gelten, was auch für Expertise in den Bereichen Steuern und Recht gilt: Was man nicht im Hause hat, muss man sich von außen holen.

Niemand sollte sich deshalb scheuen, externen Sachverstand in Anspruch zu nehmen. Das eigene Schutzniveau der Bedrohungslage anzupassen, ist alternativlos geworden. Wer jetzt konsequent handelt, investiert in die Zukunftsfähigkeit seiner Organisation. Das sollte jede Mühe wert sein.

Bild: Tim Beckmann/pixelio.de

Die wirklichen Vermögenswerte vieler Unternehmen sind für gewöhnliche Einbrecher nicht erreichbar. Sie befinden sich auf Festplatten und Servern und stehen im Fokus hochprofessioneller Täterstrukturen.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Rechtsanwalt Dr. Berthold Stoppelkamp

Bitkom-Studie: Wirtschaftsschutz 2022

Durch Diebstahl von IT-Ausrüstung und Daten, Sabotage und Spionage entsteht der deutschen Wirtschaft ein jährlicher Schaden von rund 203 Mrd. Euro. Damit wird fast jedes Unternehmen Opfer. 84 Prozent der mehr als 1.000 befragten Unternehmen aus allen Branchen waren betroffen. Dabei sind Angriffe aus Russland und China angestiegen.

www.bitkom.org

Lagebild Wirtschaftsschutz NRW 2021/22

Dieses zweite Lagebild, an dem sich über 1.000 Unternehmen beteiligt haben, kommt zu dem Schluss, dass viele Unternehmen ihren Schutz überschätzen. Die erste Datenerhebung stammt aus dem Jahre 2019. Damals lag das Schutzniveau auf einem Gesamtindex, der die Skala von 0 (sehr schlecht) bis 10 (sehr gut) umfasst, noch bei 4,81. Aktuell ist dieser Index auf 4,41 gesunken.

www.im.nrw

BKA-Lagebild Organisierte Kriminalität 2021

Die Zahl der Ermittlungsverfahren gegen kriminelle Banden ist 2021 im Vergleich zum Vorjahr um 17,2 Prozent auf 696 Verfahren angestiegen. Sorge bereitet eine immer stärkere Bewaffnung der OK-Gruppierungen, bei 7,5 Prozent wurden Waffen sichergestellt. Bei der Clankriminalität konzentrieren sich 70 Prozent der Ermittlungsverfahren auf die Bundesländer BE, NRW, HB und NI.

www.bka.de

Materialien zum Thema Desinformation

Die Russische Föderation ist bestrebt, bezüglich ihres Angriffskrieges auf die Ukraine durch Verbreitung von Desinformationen und Propaganda die öffentliche Meinung zu ihren Gunsten zu beeinflussen. Um dem entgegenzutreten, wurde von der Bundesregierung ressortübergreifend eine für die Öffentlichkeit konzipierte Handreichung „Gemeinsam gegen Desinformation" erarbeitet.

www.verfassungsschutz.de

RA Dr. Berthold Stoppelkamp

Zuständiges Geschäftsführungsmitglied für den BDSW-Arbeitskreis Wirtschaftsschutz