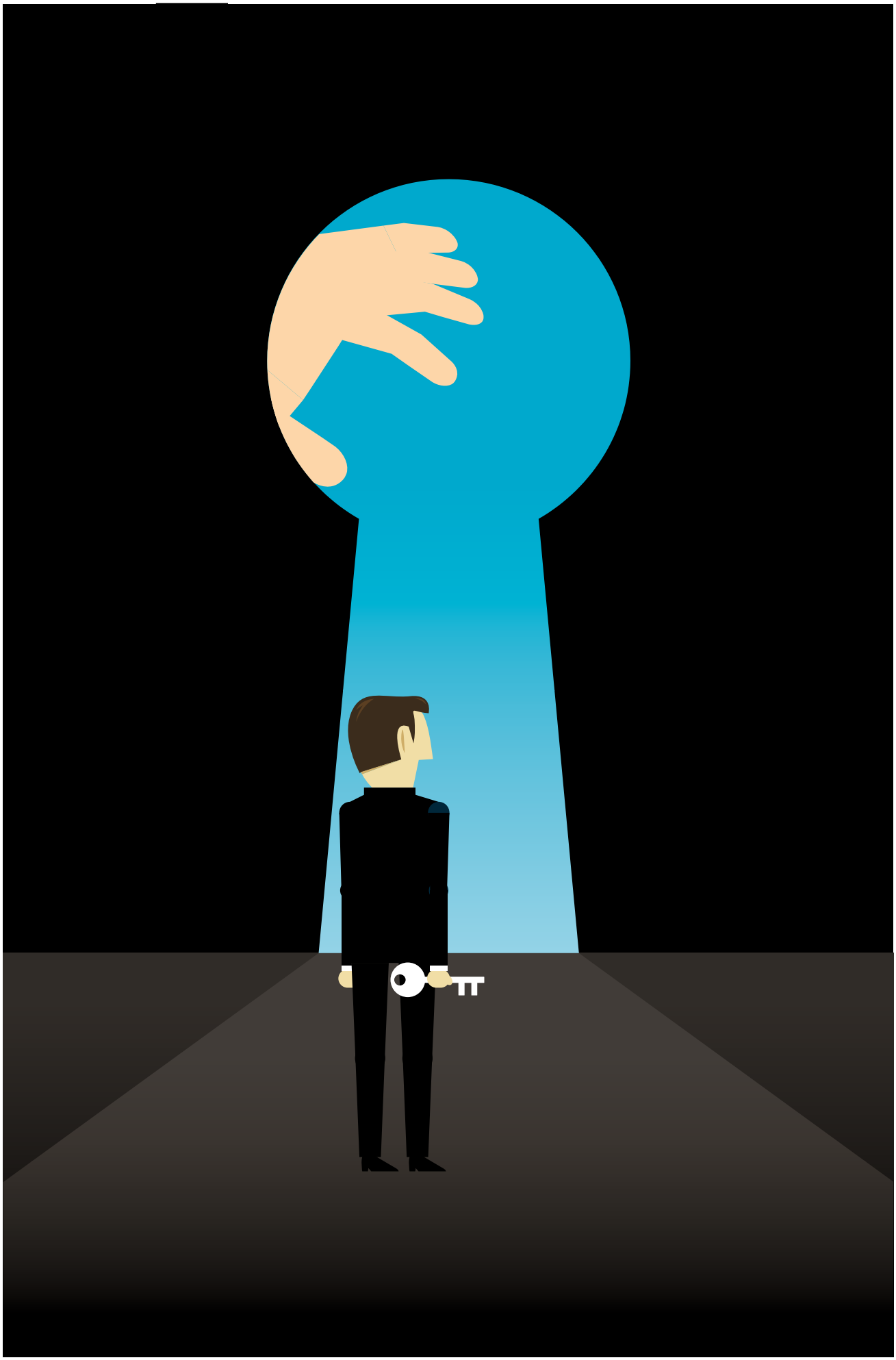

Bestellte Einbrecher

Manager, die in Sachen ***Cybersecurity*** schon alles zu wissen glauben, haben vermutlich noch nie White-Hat-Hacker engagiert. Die bezahlten Angreifer knacken IT-Systeme bevor Kriminelle es tun – und decken oft erschreckende Schwachstellen auf

Als Stefan Ellguth Entwarnung gab, hing der Haussegen schief. Richtig schief. Wochenlang hatte eine Hackerattacke die IT-Abteilung des großen deutschen Versicherers auf Trab gehalten. Was das Team nicht wusste: Sicherheitschef Ellguth, der in Wirklichkeit anders heißt, hatte die Angreifer selbst angeheuert. Über Monate forschten sie das Unternehmen aus: In Social-Media-Profilen fanden sie Informationen, mit denen sie Geschichten für Phishing-Mails erfinden konnten. Auf YouTube suchten sie Imagevideos nach Informationen über das Gebäude und die verwendete Hardware ab. Als Paketboten oder Handwerker verkleidet, versuchten sie, an Terminals heranzukommen und Wanzen zu platzieren.

Als dann der eigentliche Angriff begann, herrschte Ausnahmezustand in der IT-Abteilung. „So etwas packt die Leute bei der Berufsehre, die sitzen dann da bis in die Morgenstunden und finden kein Ende“, sagt Ellguth. Und dann, nach all dem Stress, heißt es: Entwarnung, war nur ein Test! „Das haben die mir schon krummgenommen. Jedenfalls im ersten Moment.“

„Red Team Assessment“ nennt sich ein solcher bestellter Hackerangriff. Dabei handelt es sich um eine besonders anspruchsvolle Art sogenannter Penetrationstests, bei denen vom Unternehmen bezahlte Angreifer versuchen, in die IT-Systeme des Auftraggebers einzudringen. Das können Webserver oder Firmennetze sein, aber auch Smartphones, Fabrikroboter, Webcams, kurz: alle Geräte, die mit dem Internet verbunden sind.

Schäden durch Cyberkriminalität binnen zwei Jahren verdoppelt

Attacken aus dem Cyberspace richten immer gravierendere Schäden in deutschen Unternehmen an. So musste der Kreuzfahrtanbieter Aida Cruises zum Jahreswechsel zwei Reisen kurzfristig absagen, weil Hacker die IT-Systeme der Schiffe lahmgelegt hatten. Zeitungen der Funke Mediengruppe („WAZ“, „Hamburger Abendblatt“) erschienen nach einem Cyberangriff in der Weihnachtszeit tagelang in reduziertem Umfang. Nach Berechnungen des Branchenverbands Bitkom verursachte Internetkriminalität in Deutschland 2019 Schäden von knapp 103 Milliarden Euro – fast doppelt so viel wie im vorherigen Erhebungszeitraum 2017/18.

Zugang verschaffen sich die Übeltäter über Schwachstellen im System: veraltete Software, unzureichende Sicherheitsmaßnahmen oder leichtfertige Mitarbeiter. Bestellte Cybereinbrecher arbeiten genauso – nur ohne böse Absichten wie Datendiebstahl oder Erpressung. Das Ziel der sogenannten White-Hat-Hacker oder auch „Ethical Hacker“ ist, Unternehmen ihre Sicherheitslücken vor Augen zu führen und gemeinsam mit ihnen einen Plan zu entwickeln, diese Lücken zu schließen – bevor Kriminelle sie entdecken.

„Das ist aber immer nur der erste Schritt“, sagt der Ethical Hacker Michael Wiesner. „Ich erarbeite mit meinen Kunden immer auch ein kontinuierliches Schwachstellenmanagement. Sie müssen da wirklich täglich dranbleiben und genug Personal einsetzen. Ich erlebe es zu oft, dass ich bei einem Kunden ein Jahr später immer noch dieselben Sicherheitslücken finde, weil die IT nicht hinterherkommt.“

2019 waren nur 64 Prozent der deutschen Mittelständler technisch und organisatorisch gut auf Cyberangriffe vorbereitet, ergab der Quick-Check Cybersecurity des GDV und der VdS Schadenverhütung. „Vielen ist nicht bewusst, dass es nur eine Frage der Zeit ist, bis sie gehackt werden“, sagt Christian Swoboda, Sicherheitschef der Gothaer Versicherung. „Es gibt immer ein Schlupfloch.“

Dass eine im Verborgenen arbeitende Mannschaft – das Red Team – über Monate einen Angriff vorbereitet und durchführt, während die hauseigene IT – das White Team – nichts davon ahnt, ist ein Aufwand, den sich nicht jede Firma leisten kann; bei Tagessätzen von 1800 Euro und mehr gehen die Kosten schnell in den sechsstelligen Bereich. Es geht aber auch schneller –

viel schneller „Bei Mittelständlern sind wir in der Regel zwei bis drei Tage im Einsatz“, sagt Wiesner. „Die ersten Schwachstellen finden wir meist schon nach zehn Minuten.“ Schlechte Passwörter etwa: „Ich hatte einen Kunden, bei dem mehr als die Hälfte der Benutzer noch das Initialpasswort verwendete: den Namen des Unternehmens.“

Jedes Unternehmen kann Opfer eines Hackerangriffs werden

Ein weiteres Problem: veraltete Systeme mit bekannten Sicherheitslücken, die man längst hätte patchen, also mit einem Update hätte beheben müssen. „Die WannaCry-Sicherheitslücke, wegen der 2017 bei der Bahn die Anzeigetafeln ausfielen, sehe ich immer noch bei 90 Prozent meiner Kunden auf mindestens einem Server.“ Vor allem im Maschinenbau findet Wiesner solche technischen Methusalems. In der Branche haben manche Anlagen eine Lebensdauer von 20 Jahren und mehr. Was das für die Sicherheit von Steuerungsrechnern bedeutet, ist vielen Firmen nicht bewusst.

Wie aggressiv ein Ethical Hacker vorgeht, besprechen Auftraggeber und Dienstleister vorab, ebenso die Art des Tests. Bei einem Black-Box-Test etwa bekommt der Hacker vorab keine Informationen über die Netzwerke und Systeme des Kunden, er muss selbst nach Schwachstellen suchen. Schneller geht in der Regel ein White-Box-Test, bei dem die Hacker technische Informationen bekommen und so zielgerichteter bestimmte Schwachstellen angreifen können. Voraussetzung ist stets ein gutes Vertrauensverhältnis zwischen Kunden und Dienstleister. „Wir haben uns bei der Auswahl viel Zeit gelassen“, sagt Ellguth. „Und wir verlassen uns nicht nur auf Zertifikate, sondern schauen sehr genau auf die Referenzen und den menschlichen Kontakt.“

Wo die Basis nicht stimmt, können die Dienstleister ihren Job nicht machen. „Ich sollte mal bei einem Krankenhaus einen Penetrationstest machen, hätte aber 80 Prozent der Systeme nicht anfassen dürfen“, sagt Profihacker Wiesner. „Dann kann man es auch lassen.“

IT-Sicherheit könne nur gelingen, „wenn die Geschäftsführung die

Quelle: BSI

Bedeutung des Themas erkennt und Menschen befähigt, entsprechend zu handeln“, sagt Ole Sieverding vom Versicherer Hiscox, der Cyberpolicen anbietet und den jährlichen „Cyber Readiness Report“ herausgibt. „Die Bereitschaft, sich mit dem Thema IT-Sicherheit auseinanderzusetzen, ist aber immer noch auf niedrigem Niveau. Im internationalen Vergleich ist Deutschland 2020 sogar weiter zurückgefallen.“

Der Irrglaube, wer keine wertvollen Daten oder Patente besitze, sei für Hacker uninteressant, ist nach wie vor weit verbreitet. Dabei geht es bei vielen Angriffen nicht um Datendiebstahl, sondern um Erpressung: Produktionssysteme werden durch sogenannte Ransomware lahmgelegt, die Datenbestände auf allen Servern verschlüsselt, und erst gegen Zahlung eines Lösegelds wieder freigegeben.

„Diese Gefahr ist hier erst 2016 ins öffentliche Bewusstsein gekommen, als das Lukaskrankenhaus in Neuss von einer Ransomware-Attacke lahmgelegt wurde“, sagt Sieverding. Auch der Markt für Cyberversicherungen sei zuletzt gewachsen, weil immer mehr Unternehmen verstünden, dass ein Hackerangriff sie ebenso komplett lahmlegen kann wie ein Feuer- oder ein Wasserschaden. Je nach Ausgestaltung deckt eine Cyberversicherung zudem nicht nur materielle Schäden ab, sondern stellt der Firma im Ernstfall auch einen Krisencoach zur Seite, der beim Umgang mit der Ausnahmesituation hilft – etwa bei der Frage, wie man kommuniziert, dass die Firma gehackt wurde.

Sicherheitslücken stecken oft in zugekauften Komponenten

Der GDV plädiert für mehr Transparenz im Umgang mit Cyberangriffen. „IT kann nie zu 100 Prozent sicher sein. Wichtig ist, dass man Krisen bewältigt und Mängel beseitigt und nicht so tut, als ob sie nicht da wären“, sagt Patrik Maeyer, Leiter des Krisenreaktionszentrums der Versicherungsbranche (LKRZV). Seit 2010 gibt das LKRZV rund um die Uhr Sicherheitswarnungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) an die Versicherer weiter, sodass diese innerhalb von 30 Minuten auf jede neue Bedrohungslage reagieren können.

Umgekehrt melden Versicherer über die LKRZV-Plattform Cyberangriffe an das BSI weiter. „Wenn es keine meldepflichtigen Fälle sind, können die Unternehmen die Informationen auch anonymisiert weitergeben lassen“, sagt Maeyer. „Das ist sehr wichtig, weil es den Firmen die Hemmung nimmt, auch bei niederschwelligen Vorfällen schon Signale zu senden. Wir haben außerdem vor drei Jahren eine Initiative gestartet, bei Cyberangriffen auch die Staatsanwaltschaften einzubinden und in die Notfallpläne einzubeziehen.“

Trotz des wachsenden Problembewusstseins tun sich viele Unternehmen nach wie vor schwer, transparent mit dem Thema Cybersecurity umzugehen. Zu groß ist die Angst vor einem Imageschaden, falls Sicherheitslücken auftreten. Manche unterdrücken sogar aktiv die Bemühungen ethischer Hacker. „Wir erleben es oft, dass Firmen ein Problem erst einmal leugnen, wenn wir ihnen sagen: Euer Gerät ist unsicher“, sagt Johannes Obermaier vom Fraunhofer-Institut für angewandte und integrierte Sicherheit (AISEC).

Die Forscher testen die Sicherheit von IT-Hardware meistens im Kundenauftrag, oft aber auch aus wissenschaftlichem Interesse. Viele Penetrationstests im Fraunhofer AISEC beginnen auf der Werkbank: „Wir schrauben das Gerät auf und schauen uns an, welche Komponenten darin verbaut sind. Kommt mir irgendetwas bekannt vor? Kann ich den Speicher auslesen und daraus Erkenntnisse ziehen, wie das System aufgebaut ist? Finde ich Angriffspunkte, mit denen ich zum Beispiel die Kontrolle übernehmen, in die Firmencloud vordringen oder das Gerät für mein Botnetz kapern kann?“

Penetrationstests sind in der Lage, Sicherheitsmängel aufzudecken, die aus den Konstruktionsplänen nicht hervorgehen. „In praktisch jedem Gerät stecken zugekaufte Komponenten und Software, in denen Sicherheitslücken stecken können. Denken Sie nur an all die Steuergeräte in einem modernen Auto“, sagt Obermaier. Es könnten Missverständnisse beim Zulieferer auftreten oder Komponenten ohne übergreifendes Sicherheitskonzept zusammengefügt werden. Tritt ein Sicherheitsproblem zutage, sollten sich Firma und Forscher zusammensetzen und gemeinsam nach einer Lösung suchen, rät der Sicherheitsexperte.

Auf diese Weise hätten bei Stefan Ellguths Arbeitgeber auch das Red Team und das White Team zusammengefunden und den gesamten Angriff durchgesprochen, sagt der Sicherheitschef: „Hinterher haben alle gesagt: ‚Klasse, das machen wir noch mal!‘“

20.000	117,4	35.000	7
Bot-Infektionen täglich	**Millionen neue Schadprogramme 2020**	**Mails mit Schadprogrammen pro Monat abgefangen**	**Millionen Warnmeldungen des BSI**