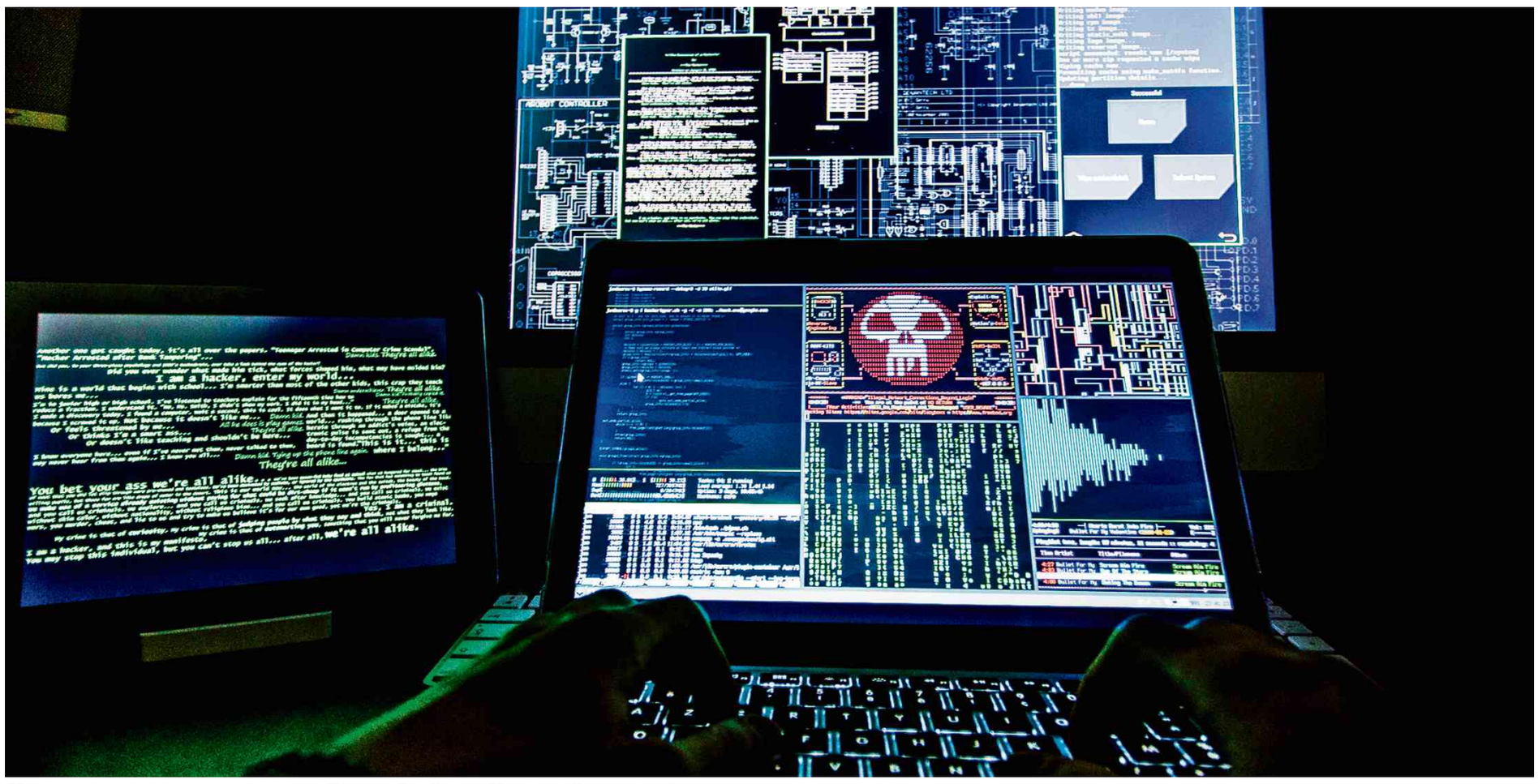

Hacker gehen bei ihren Angriffen auf Firmen, Behörden, Krankenhäuser oder Stromversorger immer raffinierter vor. Foto: Reporters/STG/laif

Katastrophen auf Bestellung

Cyberkriminalität Die SySS ist Marktführer in Deutschland, wenn Firmen, Behörden und Versorger Hackerangriffe simulieren lassen wollen. Bei Geschäftsführer Sebastian Schreiber fragten sogar Geheimdienste an. Ein Einblick in die aktuelle Bedrohungslage. *Von Daniel Gräfe*

Für Sebastian Schreiber sind Katastrophenszenarien Alltag geworden, schließlich ist er ein Teil davon. Doch für die Firmen, Behörden, Krankenhäuser oder Stromversorger, die ihn beauftragen, um die Sicherheit ihrer IT-Systeme testen zu lassen, sind sie oft ein Schock. Wenn Schreiber und sein Team sich von außen wie Hacker in die Systeme geschlichen haben, folgt manchmal der alarmierende Befund: „In vielen Situationen wären wir in der Lage gewesen, den Strom abzustellen, Patientendaten zu verschlüsseln, bei einem Pumpspeicherkraftwerk den Speichersee zu leeren oder Industrieroboter fehlerhaft arbeiten zu lassen“, sagt Schreiber.

Foto: SySS

„Wir hätten den Strom abstellen und Patientendaten verschlüsseln können.“

Sebastian Schreiber, Chef des IT-Dienstleisters SySS

Seine Aussagen haben so viel Gewicht, weil die SySS bei den Penetrationstests, wie die Hackerangriffe auf Auftrag genannt werden, in Deutschland als Marktführer gilt. Zu den Unternehmenskunden zählen Autohersteller, Maschinenbauer, Pharma-, Chemie- und Telekommunikationsfirmen, Banken, Versicherungen, Mischkonzerne. Zwei Drittel der 30 Dax-Unternehmen sind darunter, aber auch kleine Betriebe, große wie kleine Stromversorger, Ministerien, Krankenhäuser, Behörden.

Die meisten Kunden kommen aus dem Südwesten, etliche melden sich immer wieder. „Die Notfalleinsätze häufen sich“, sagt Schreiber. Jüngst wurden eine große Bäckereikette und eine Arztpraxis aus Stuttgart gehackt. Sehr selten macht ein Unternehmen einen Angriff transparent, wie die Tübinger Buchhandelskette Osiander, die es vor einigen Monaten erwischte.

Dann geht es ganz schnell. In Krisensituationen muss die Geschäftsführung wie bei einem Feuerwehreinsatz Kompetenzen abgeben, damit der Angriff abgewehrt werden kann. Dann mahnt Schreibers Einsatzgruppe zur Ruhe, identifiziert die Verantwortlichen, sammelt Informationen, analysiert, sucht nach Lösungen. Der Kunde entscheide dabei, wie stark das Einsatzteam die Kontrolle übernehme oder vor allem berate, betont Schreiber. „Das kommt auch darauf an, ob die Produktion still steht oder ein Unternehmen nicht an die Personaldaten kommt.“ 2000 Euro pro Person und Tag koste ein Notfalleinsatz. Am Ende wird das Back-up, also die zuletzt komplett gespeicherten Daten, eingespielt. Auch wenn die Maschinen wieder laufen – eine Sicherheit, dass der Angreifer komplett zurückgedrängt wurde, gebe es nicht. „Das ist wie mit den Metastasen bei einer Krebserkrankung. Da muss man die Ergebnisse regelmäßig wieder überprüfen.“

Am häufigsten seien derzeit sogenannte Ransomware-Angriffe, also Trojaner, die Daten verschlüsseln und für deren Entschlüsselung die Angreifer Lösegeld verlangen, sagt Schreiber. Das bestätigen auch das Landeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik (BSI) unserer Zeitung – dabei habe die Zahl der registrierten Hackerangriffe in den vergangenen Jahren generell stark zugenommen.

Oft beginnt eine Ransomware-Attacke damit, dass ein Mitarbeiter einen infizierten E-Mail-Anhang öffnet. Die Absender gehen dabei immer raffinierter vor. Zum Beispiel erhält ein Angestellter eine Antwort auf einen früheren Mailwechsel mit einem Geschäftskunden samt Hinweis auf einen aktuellen, beigefügten Auftrag. Doch nach dem Öffnen ist nur der Lösegeldhinweis samt verschlüsselter Festplatte zu sehen. Als Vorbereitung hatte der Angreifer zum Beispiel das Postfach eines Geschäftskunden geknackt und Kontakte und den Mailverkehr ausgelesen. „Die Legenden der Angreifer sind nahezu perfekt. Auch ich hätte schon beinahe auf einen Anhang geklickt“, sagt Schreiber.

Ein weiterer Trend: Die Angreifer wissen die infizierten Computer besser zu nutzen. Oft agieren sie über längere Zeit behutsam im Verborgen, um sich tiefer ins Firmennetz vorzuarbeiten. „Die Angreifer agieren so, wie früher die staatlichen Akteure gehackt haben“, sagt Schreiber. Die kurzfristigen Ziele gebe es allerdings nach wie vor. Angreifer verbinden infizierte Rechner zu sogenannten Bot-Netzen, um mit massenhaften Angriffen zum Beispiel Firmenserver lahmzulegen. Sie nutzen die Rechenleistung für das Schürfen von digitalen Währungen. Oder sie verschlüsseln Rechner auch mal weniger gezielt und massenhaft, um auf die Schnelle möglichst viel Geld zu erpressen.

Aus seiner Praxis wisse er, dass der Rat der Kriminalämter, kein Lösegeld zu zahlen, kaum beherzigt werde, sagt Schreiber. „Viele Unternehmen überweisen das Lösegeld sehr schnell, um wieder arbeitsfähig zu sein, insbesondere, wenn das geforderte Lösegeld im Vergleich zur Bedrohung niedrig ist.“

Schreiber zeigt Verständnis dafür, dass nicht immer die hochwertigste Software eingesetzt werde. Denn diese koste neben Geld auch Zeit. „Wer eine hohe Qualität will, würde den Wettlauf um die Digitalisierung aufgeben. Jeder nutzt Software, Betriebssysteme und Protokolle, die nicht immer funktionieren. Mir fällt es schwer, meine Kunden auf einen strengen Sicherheitskurs zu bringen, weil eine hochwertige IT andere Ziele torpediert“, so Schreiber. Konzerne seien dabei nicht besser gegen Angriffe gerüstet als kleine oder mittelständische Firmen. „Die Konzerne haben zwar mehr Geld und Mitarbeiter, aber auch eine viel komplexere IT.“

Am Ende bleibt es damit für jeden ein Wettlauf, Sicherheitslücken wieder zu stopfen, bis neue erkannt oder ausgenutzt werden. Ein Wissensvorsprung, kann da von Vorteil sein. Wohl auch deshalb hat Schreiber schon Anfragen von Geheimdiensten außerhalb Europas erhalten, klassisch per Mail. „Sie schreiben, dass sie unsere Veröffentlichungen gelesen haben und gerne Beratungen oder Schulungen einkaufen würden“, sagt Schreiber – und betont: „Das sagen wir natürlich ab.“

GEMELDETE ANGRIFFE

Landeskriminalamt Die Zentrale Ansprechstelle Cybercrime im Landeskriminalamt hat im ersten Halbjahr dieses Jahres 541 Kontaktaufnahmen wegen Sicherheitsvorfällen hauptsächlich von Firmen registriert, im Vorjahreszeitraum waren es nur 152 gewesen.

BSI Das Bundesamt für Sicherheit in der Informationstechnik verzeichnete im zweiten Halbjahr 2018 bundesweit 157 Meldungen aus dem Bereich der kritischen Infrastruktur wie Energie, Wasser, Ernährung und Gesundheit – das ist mehr als in den zwölf Monaten zuvor. Grund einer Meldung kann, muss aber nicht ein Hackerangriff sein. (dag)

Daimler steigt bei Carwow ein

Investition Die Beteiligung an der Autokauf-Webseite soll dem Konzern Kundendaten liefern.

Mercedes-Hersteller Daimler investiert viel Geld in die Autokauf-Website Carwow. Der Autokonzern führt die 28 Millionen Euro schwere jüngste Finanzierungsrunde des Start-ups an. Carwow will mit dem Geld vor allem das Geschäft in seinen bisherigen Märkten Großbritannien, Deutschland und Spanien ausbauen. Neben Daimler nahmen auch mehrere deutsche Autohändler an der Finanzierungsrunde teil. Bei Carwow können Nutzer ein Fahrzeug auswählen und werden dann zu Händlern in ihrer Nähe weitergeleitet.

Die Branche muss gerade ihre Geschäftsmodelle daran anpassen, dass vor allem Einwohner von Städten weniger Autos kaufen und die Markentreue viel niedriger ist als früher. Zudem könnte die Industrie auf eine Zukunft mit selbstfahrenden Robotaxis zusteuern, in der der Autoabsatz sinkt und das Geld stattdessen vor allem mit dem Betrieb der Fahrdienste verdient wird.

Daten von Carwow gäben Autoherstellern einen Einblick in den Entscheidungsprozess der Käufer, den sie sonst nicht hätten, sagte der Chef von Carwow Deutschland, Philipp Sayler von Amende. „Wir sehen, welche Wettbewerbs-Fahrzeuge hat der Kunde konfiguriert, welche Fahrzeuge hat er beim Händler tatsächlich angefragt und was hat er am Ende zu welchem Preis gekauft.“ Im Schnitt konfiguriere ein Nutzer bei der Auswahl vier Modelle von drei Marken. Daimler-Manager Axel Harries, der Verkaufschef bei Mercedes-Benz Cars ist, wird Mitglied des Verwaltungsrates von Carwow. Die Plattform sei offen dafür, in späteren Finanzierungsrunden weitere Autohersteller aufzunehmen, sagte Sayler von Amende. Carwow war 2012 in Großbritannien gestartet, kam 2016 nach Deutschland und startete 2018 in Spanien. *dpa*

Kontakt

Wirtschaftsredaktion
Telefon: 07 11/72 05-12 11
E-Mail: wirtschaft@stzn.de