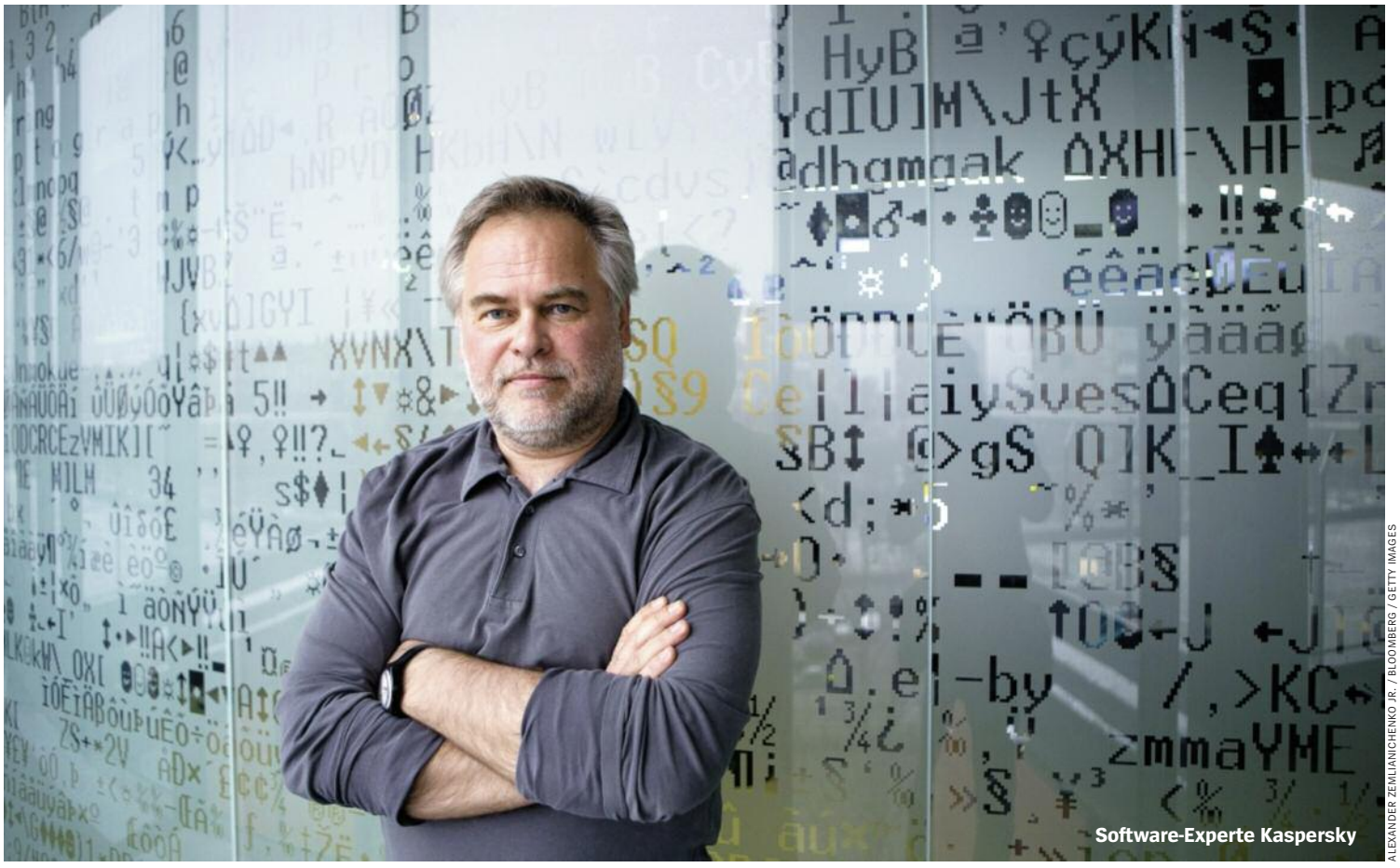

Software-Experte Kaspersky

ALEXANDER ZEMLIANICHENKO JR. / BLOOMBERG / GETTY IMAGES

„Wir leben im Cyber-Mittelalter“

Sicherheit Der russische IT-Unternehmer Eugene Kaspersky über Hackerangriffe auf Autos, Seehäfen, den „Islamischen Staat“ – und seine eigene Firma

Kaspersky, 50, ist Gründer und Chef des Moskauer Softwareunternehmens Kaspersky Lab. Verbrauchern ist Kaspersky vor allem durch seine gleichnamigen Antivirus-Programme bekannt. Seine Experten trugen aber auch maßgeblich zur Analyse aufwendiger Cyberwaffen wie „Stuxnet“ und „Duqu“ bei und unterstützen Behörden bei der Jagd nach Onlinekriminellen.

SPIEGEL: Herr Kaspersky, Autos lassen sich von Hackern fernsteuern, Fernseher können Wohnzimmer ausspionieren. Werden wir durch die zunehmende Vernetzung aller Dinge angreifbarer?

Kaspersky: Computer und ihre Vernetzung machen mein Leben als Privatmann – und übrigens auch das als Unternehmer – besser, bunter und effizienter. Sie produzieren insgesamt auch weniger Fehler als wir, der Homo sapiens ist ein sehr altes und anfälliges System. Rechner haben allerdings auch Schwächen und sind verwundbar. Wenn Hacker mit einem einfachen Laptop ein Auto in den Graben steuern können, haben wir ein Problem. Im Transportwesen geht es um Menschenleben. Bis die ersten selbstfahrenden Autos unterwegs sind, muss man das spätestens im Griff haben.

SPIEGEL: Wäre das nicht ein bisschen spät?

Kaspersky: Ich fürchte, es ist realistisch. Die Steuerungssysteme, die heute im Einsatz sind, wurden entwickelt, als es derart ausgefeilte Angriffe noch nicht gab. Die Produktzyklen für Automodelle betragen viele Jahre. Sie können auf eine unsichere Basis nicht einfach Sicherheit aufsetzen, sie muss künftig von Beginn an eingebaut sein, „by design“ sozusagen. Noch leben wir im Cyber-Mittelalter, die wirklich kritischen Systeme müssen wir redesignen oder neu erfinden. Das wird ein schwerer Weg, denn wer als Hersteller heute der Sicherheit eine zu hohe Priorität einräumt, produziert zu teuer und zu langsam, er wird den Wettbewerb verlieren und deshalb immer Kompromisse machen.

SPIEGEL: Das klingt nicht gerade beruhigend, zumal im Frühjahr ein amerikanischer IT-Experte behauptete, die Steuerungssysteme einer Boeing auf einem Linienflug manipuliert zu haben.

Kaspersky: Anders als im Fall der Autos gibt es dafür keine Beweise. Es ist ohne große Probleme möglich, die Bord-Unterhaltungsangebote zu knacken. Aber die sind eigentlich von den kritischen Steuerungssystemen getrennt. Im Flugverkehr sind es bislang eher klassische Computerfehler, die für Probleme sorgen. 2008 stürzte auch deshalb eine Spanair-Maschine kurz nach dem Start ab. Erst Anfang des Monats musste der Flughafen Paris-Orly geschlossen werden, weil eine Wetter-Software streikte – dabei kam heraus, dass dort noch das total veraltete System Windows 3.1 im Einsatz war.

SPIEGEL: Ihr Unternehmen beschäftigt sich derweil bereits mit Zukunftsszenarien, in denen sogar Körper vernetzt werden. In Berlin haben Sie unlängst zusammen mit „Biohackern“ einen Mikrochip vorgestellt, der Menschen unter die Haut implantiert werden kann – damit soll man einmal bezahlen und ohne Schlüssel Türen öffnen können. Wann erleben wir den ersten gehackten Menschen?

Kaspersky: Bei diesen Chips geht es noch um recht simple Prototypen, aber die Entwicklung wird sich nicht aufhalten lassen, und die Implantate werden immer smarter. Es ist nach den Wearables wie der Apple Watch einfach der nächste logische Schritt. Und es gibt schon heute medizinische Implantate, bei denen ich das Risiko sehe, dass zumindest deren Daten kompromittiert

werden. Ich gebe aber zu: Selbst würde ich mir eher keinen Chip einpflanzen lassen und hoffe auch, das nicht mehr zu erleben. Aber es wird kommen, da bin ich sicher.

SPIEGEL: Von der Science-Fiction zu Ihrem Tagesgeschäft – welche Trends beobachten Sie bei der Onlinekriminalität?

Kaspersky: Sie wird immer professioneller, mit der einfachen Online-Straßenkriminalität, die auf Gelegenheiten für simple Diebstähle lauerte, hat das nichts mehr zu tun. Bis vor Kurzem konnten wir noch klar unterscheiden zwischen den Werkzeugen von Kriminellen und den Spionagetools von Staaten. Das verschwimmt nun leider zusehends. Zudem hat das organisierte Verbrechen das Netz für sich entdeckt und heuert Hacker für seine Zwecke an.

SPIEGEL: Haben Sie konkrete Beispiele?

Kaspersky: Ein Drogenkartell hat Hacker dazu gebracht, die Verladelogistik im Seehafen von Antwerpen zu infiltrieren. So konnten sie die aktuellen Standorte der Drogencontainer genau verfolgen und schließlich damit verschwinden. Auch in einer Kohlenmine wurde das System der Betreiber gehackt. Anschließend spuckte es falsche Gewichtsangaben aus, und die Kriminellen konnten riesige Mengen an Kohle beiseiteschaffen und auf eigene Rechnung verkaufen.

SPIEGEL: Gibt es auch Beispiele dafür, dass Terroristen das Netz für Cyberanschläge nutzen?

Kaspersky: Ich fürchte, wenn die Mafia talentierte Hacker für ihre Zwecke anheuern kann, dann können islamistische Terroristen das auch.

SPIEGEL: Die Anonymous-Bewegung hat dem IS den Krieg im Netz erklärt. Was halten Sie davon?

Kaspersky: Nicht viel. Bislang sehe ich vom IS im Netz vor allem Websites und viele Social-Media-Accounts, über die er seine Propaganda betreibt. Das sollten staatliche Behörden und soziale Netzwerke eigentlich selbst in den Griff bekommen, dafür braucht es Anonymous doch nicht, come on!

SPIEGEL: Ihr Unternehmen machte vor einigen Monaten weltweit Schlagzeilen, als es einen Bericht über die Carbanak-Gruppe veröffentlichte. Sie hat demnach bis zu eine Milliarde Dollar in Banken, am Devisenmarkt und sogar in Kasinos in Las Vegas erbeutet – und unbemerkt auf eigene Konten in den USA und China transferiert. Was ist seit dem Bericht passiert?

Kaspersky: Wir wissen inzwischen, dass ein Konglomerat von internationalen Onlinekriminellen dahintersteckt, von denen leider auffallend viele Russisch sprechen. Die schlechte Nachricht ist, dass es Carbanak immer noch gibt. Allerdings gibt es auch eine gute: Die russische Polizei und die zuständige Abteilung des Inlandsgeheimdienstes haben in den letzten Monaten zahlreiche mutmaßliche Täter verhaftet. In einem Fall fanden sie dabei einen Raum vor, dessen Boden komplett mit Rubel- und Dollarpaketen bedeckt war. Mehr darf ich dazu leider nicht sagen, weil die Ermittlungen noch laufen.

SPIEGEL: Deutsche Banken kritisierten Ihren Report scharf, weil Sie auf einer Karte Deutschland als stark betroffen darstellten. Sie würden zu Werbezwecken Verunsicherung schüren, dabei seien deutsche Banken gar nicht betroffen, hieß es.

Kaspersky: Wir haben in der Karte klar benannt, dass es um deutsche IP-Adressen geht, die von Carbanak betroffen waren. Dabei bleiben wir auch. Es bringt nichts, diese Probleme wegzudiskutieren. Wir können diese Adressen aber nicht bestimmten Organisationen zuordnen. Das ist Sache der Strafverfolgungsbehörden.

SPIEGEL: US-Unternehmen setzen zunehmend darauf, Angreifer selbst auszuschalten. Ein Bericht empfahl dem Kongress, solche „hack backs“ von Konzernen zu erlauben. Was halten Sie davon?

Kaspersky: Das ist ein brandgefährlicher Kurs, den ich nicht einschlagen würde. Ich halte so eine Erlaubnis nur für Fälle denkbar, in denen ein Unternehmen aus dem Inland attackiert wird – nur dafür kann ein nationaler Gesetzgeber das eigentlich legalisieren. Die meisten Angriffe werden aber über Grenzen hinweg geführt. Dazu kommt das Problem, dass es Standard ist, falsche Fährten zu legen. Was ist, wenn ein solcher „hack back“ Unschuldige trifft? Das könnte leicht einen Wirtschaftskrieg auslösen.

SPIEGEL: In diesem Jahr hat Sie etwas ereilt, was in Ihrer Branche nicht die beste Werbung ist. Kaspersky wurde selbst gehackt. Ganz schön peinlich, oder?

Kaspersky: Das ist keine Schande, im Gegenteil, das kann jeder Firma und jeder Institution passieren – nur würde außer uns wohl niemand einen derart ausgefeilten Angriff selbst entdecken. Die Angreifer wussten jedenfalls, mit wem sie es zu tun hatten. Sie haben extrem viel Zeit und Geld in die Attacke investiert, mehrere Millionen in ihrer Landeswährung …

SPIEGEL: … also wohl israelische Schekel, denn Sie haben den gleichen ausgefeilten Angriff auch in den Hotels ausgemacht, in denen die Iran-Atomgespräche stattfanden, und auch weitere Ziele deuten auf strategische Interessen Israels.

Kaspersky: Es waren jedenfalls definitiv keine Russen. Sie haben sich auch nur für die Arbeit unserer Spezialisten im Virenlabor interessiert und die jener Kollegen, die für uns Spionagesoftware analysieren. Es ging nicht um Kundendaten, unsere Finanzen oder E-Mails. Das hatte eindeutig einen politischen Hintergrund. Als hätte beispielsweise jemand nachsehen wollen, ob wir gerade sein Angriffsarsenal enttarnen.

SPIEGEL: Auch die geopolitische Situation hat Ihren Geschäften in diesem Jahr sicherlich nicht geholfen. Sie sind ein russisches Unternehmen und arbeiten eng mit der Polizei und dem Inlandsgeheimdienst FSB zusammen.

Kaspersky: Wir kooperieren mit Sicherheitsbehörden weltweit, und ja, wir mögen ein paar Verträge verloren haben, aber das waren nicht viele. Unsere wichtigsten Märkte sind in Westeuropa, und da hatten wir in diesem Jahr ein ganz anderes Problem – der Dollarwechselkurs hat unser Wachstum dort fast aufgefressen. Wir berichten in Dollar, bezahlen aber in Euro.

Interview: Marcel Rosenbach

* Aktivist bei der Verkündung einer Kriegserklärung an den IS nach den Anschlägen in Paris.

REUTERS

Anonymous-Video*: „Das sollten staatliche Behörden selbst in den Griff bekommen“