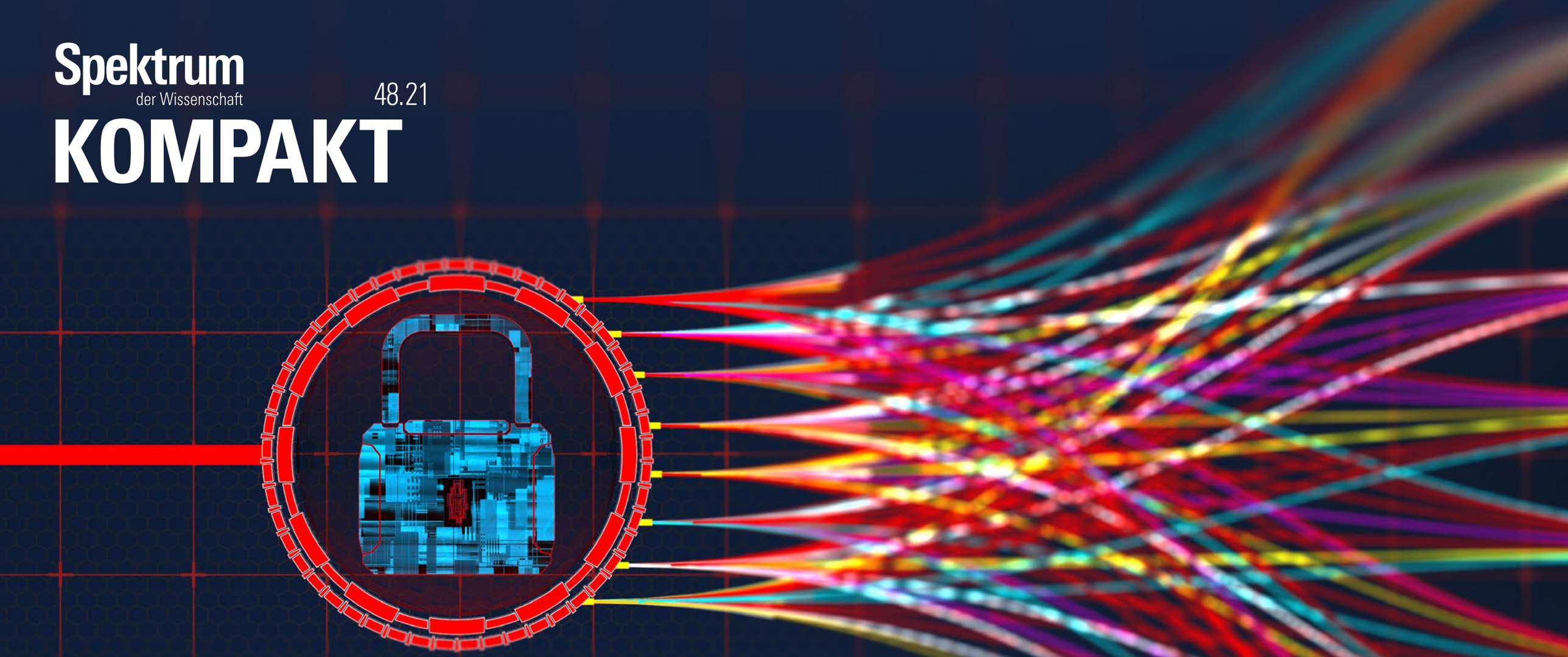
Spektrum der Wissenschaft
48.21
KOMPAKT



# KRYPTOGRAFIE

## SICHER KOMMUNIZIEREN

**Hackerangriffe**
Unsere verwundbare IT-Infrastruktur

**Datenschutz**
Die Kunst des guten Passworts

**Messenger**
Wie sicher sind Telegram und Co?

# EDITORIAL

Folgen Sie uns:

Manon Bischoff
E-Mail: m.bischoff@spektrum.de

## Liebe Leserinnen und Leser,

immer wieder hört man von Hackerangriffen, sei es, um geheime Informationen abzugreifen, Institutionen zu erpressen oder Unternehmen gezielt zu schaden. Zudem sollen künftige Quantencomputer die gängigen Verschlüsselungen, auf denen bislang viele Sicherheitssysteme basieren, knacken können. Daher tüfteln Informatikerinnen und Informatiker auf der ganzen Welt an neuartigen kryptografischen Verfahren, die sensible Daten zuverlässig schützen sollen.

Doch auch als einzelner Nutzer drängen sich angesichts der rasanten Entwicklungen in dem Bereich einige Fragen auf: Wie sicher sind die Programme, die ich verwende? Und wie gut sind meine Passwörter? Nach der Recherche habe ich jedenfalls meine Zugangscodes geändert – ich bin gespannt, ob es Ihnen genauso ergeht.

Eine spannende Lektüre wünscht Ihnen herzlich,

Erscheinungsdatum dieser Ausgabe: 06.12.2021

# IMPRESSUM

**CHEFREDAKTION:** Dr. Daniel Lingenhöhl (v.i.S.d.P.)
**REDAKTIONSLEITUNG:** Alina Schadwinkel (Digital), Hartwig Hanser (Print)
**CREATIVE DIRECTOR:** Marc Grove
**LAYOUT:** Oliver Gabriel, Marina Männle
**SCHLUSSREDAKTION:** Christina Meyberg (Ltg.), Sigrid Spies, Katharina Werle
**BILDREDAKTION:** Alice Krüßmann (Ltg.), Anke Lingg, Gabriela Rabe
**REDAKTION:** Antje Findeklee, Dr. Michaela Maya-Mrschtik
**VERLAG:** Spektrum der Wissenschaft Verlagsgesellschaft mbH, Tiergartenstr. 15–17, 69121 Heidelberg, Tel.: 06221 9126-600, Fax: 06221 9126-751; Amtsgericht Mannheim, HRB 338114, USt-IdNr.: DE229038528
**GESCHÄFTSLEITUNG:** Markus Bossle
**MARKETING UND VERTRIEB:** Annette Baumbusch (Ltg.), Michaela Knappe (Digital)
**LESER- UND BESTELLSERVICE:** Helga Emmerich, Sabine Häusser, Ilona Keith, Tel.: 06221 9126-743, E-Mail: service@spektrum.de

**BEZUGSPREIS:** Einzelausgabe € 4,99 inkl. Umsatzsteuer

**ANZEIGEN:** Wenn Sie an Anzeigen in unseren Digitalpublikationen interessiert sind, schreiben Sie bitte eine E-Mail an anzeigen@spektrum.de.

# INHALT


GORODENKOFF / GETTY IMAGES / ISTOCK


ANYABERKUT / GETTY IMAGES / ISTOCK


CARLOSCASTILLA / GETTY IMAGES / ISTOCK


DEEPBLUE4YOU / GETTY IMAGES / ISTOCK


04 HACKERANGRIFFE
Deutschlands »extrem verwundbare« IT-Infrastruktur

12 DATENSCHUTZ
Wie sicher sind Telegram und andere Messenger?

20 MATHEMATISCHE UNTERHALTUNGEN
Die Kunst des guten Passworts

29 QUANTENMECHANIK
Der schnellste Zufallszahlengenerator, der je gebaut wurde

32 OBFUSKATION
Der Heilige Gral der Informatik

45 QUANTENKRYPTOGRAFIE
Wettlauf gegen den großen Codeknacker

52 VERSCHRÄNKTE PHOTONEN
Mit Quantenschlüsseln ein Geheimnis bewahren

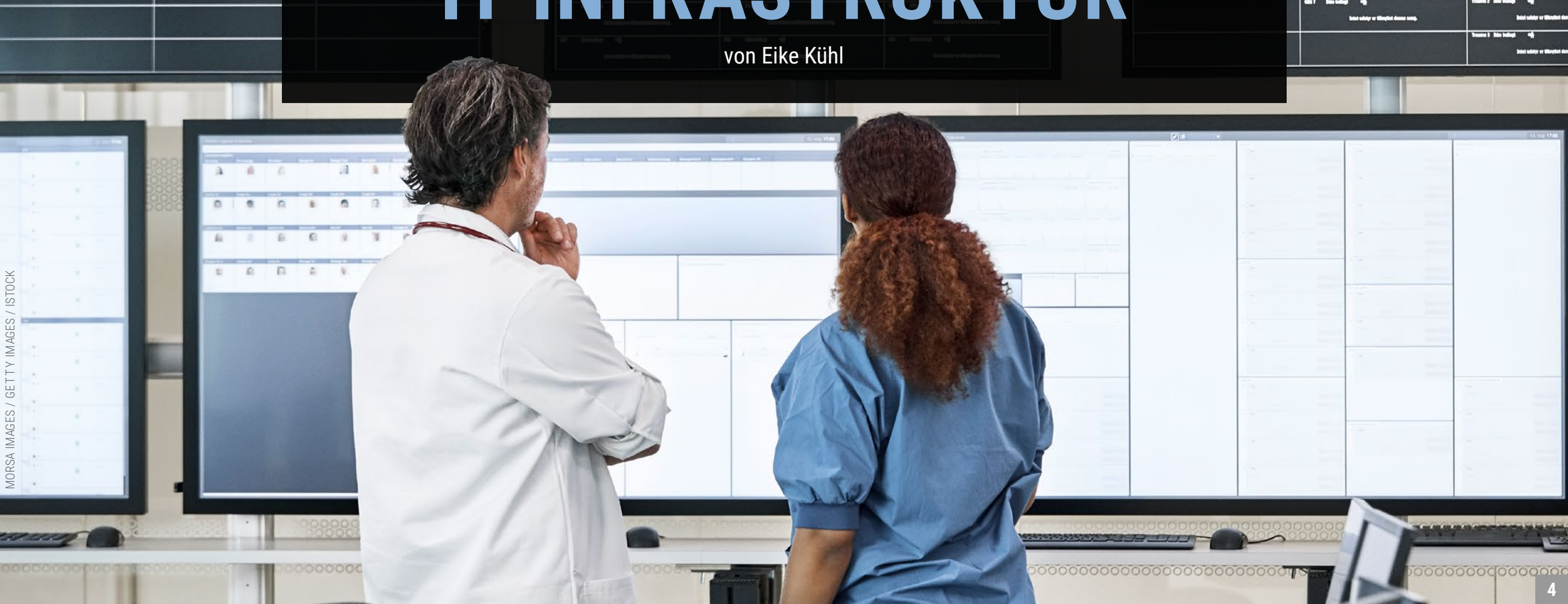
54 QUANTENKOMMUNIKATION
Drohnen bilden fliegendes Quantennetzwerk

56 INTERVIEW
Von der Kryptografie zum Weltfrieden

HACKERANGRIFFE

# DEUTSCHLANDS »EXTREM VERWUNDBARE« IT-INFRASTRUKTUR

von Eike Kühl



MORSA IMAGES / GETTY IMAGES / ISTOCK

Hacker greifen gezielt da an, wo es weh tut. Denn dort sitzen die lukrativsten Opfer. Das müsste jetzt getan werden, um Unternehmen und Behörden besser zu schützen.

Katastrophenfall, das klingt dramatisch. Das klingt nach Hochwasser und Waldbränden, nach Reaktorunfällen, Flugzeugabstürzen und Terroranschlägen. Im Landkreis Anhalt-Bitterfeld steht der Begriff seit dem Sommer 2021 für ein weiteres Szenario: einen Hackerangriff. In der ersten Juliwoche ging in der Verwaltung des Landkreises praktisch nichts mehr; keine E-Mails, keine KFZ-Zulassungen, kein Begleichen von Sozialleistungen. Um besser reagieren zu können und Hilfe von anderen Stellen anzufordern, rief der Landrat am 9. Juli schließlich den ersten Cyberkatastrophenfall in der Geschichte Deutschlands aus. Glaubt man Experten, wird es nicht der letzte gewesen sein.

Mindestens 100 deutsche Ämter, Regierungsstellen, landeseigene Kliniken, Stadtverwaltungen und Gerichte sind in den vergangenen sechs Jahren Opfer von Hackerangriffen geworden, fand unlängst eine Recherche des Bayerischen Rundfunks und von »ZEIT ONLINE« heraus. Zuletzt traf es Mitte Juli das Klinikum Wolfenbüttel. Fast immer nutzen die Angreifer so genannte Ransomware: Schadsoftware, die über Sicherheitslücken oder eine infizierte Datei eingeschleust wird und Computer und Daten verschlüsselt – so lange, bis die Opfer bereit sind, das geforderte Lösegeld zu zahlen.

In Wirtschaft und Forschung sieht es nicht besser aus. Eine aktuelle Studie des IT-Branchenverbandes Bitkom kommt zu dem Ergebnis, dass 86 Prozent der befragten Unternehmen im vergangenen Jahr Schäden durch Cyberangriffe erlitten haben. In diesem Jahr traf es unter anderem die Madsack Verlagsgruppe und den Autozulieferer EDAG, zu Beginn des Jahres zog der Angriff auf das Unternehmen SolarWinds weltweite Kreise, und vergangenen Sommer standen gleich mehrere deutsche Supercomputer, Universitäten und Forschungsinstitute im Visier. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beurteilt in seinem jüngsten Jahresbericht die Lage der IT-Sicherheit in Deutschland als »nach wie vor sehr angespannt«.

## Professionelle Cyberangriffe treffen auf anfällige Infrastruktur

»Die Beispiele der letzten Wochen und Monate zeigen, dass wir extrem verwundbar sind«, sagt Michael Wiesner,

**Eike Kühl** ist freier Journalist für Digital- und Wissenschaftsthemen.

# Glossar: Beliebte Cyberangriffe

**Zero-Day**
Hierbei handelt es sich um Sicherheitslücken, für die es zum Zeitpunkt des Angriffs noch keine Gegenmaßnahme gibt. Entwickler haben keine Zeit (»null Tage«, »zero days«), die Nutzer zu schützen. Hacker halten Zero-Day-Lücken meist lange geheim oder verkaufen sie für viel Geld, zum Beispiel an staatliche Akteure. Sie gelten als eine der mächtigsten Waffen im Cyberkrieg.

**Advanced Persistent Threats**
Bei APTs handelt es sich um zielgerichtete Cyberangriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Solche Angriffe, wie etwa auf den Deutschen Bundestag, sind häufig sehr spezialisiert und deshalb schwer zu entdecken.

**Backdoor**
Ein Backdoor (Hintertür) ist ein üblicherweise durch Viren, Würmer oder einen Trojaner installiertes Programm, das Dritten einen unbefugten Zugang zu einem Computer verschafft. Um Backdoors einzuschleusen, werden häufig Sicherheitslücken und Schwachstellen ausgenutzt.

**Botnetz**
Als Botnetz wird ein Verbund aus zahlreichen Rechnern bezeichnet, die allesamt von einem fernsteuerbaren Schadprogramm (Bot) befallen sind. Der Botnetz-Betreiber kontrolliert den Rechnerverbund von zentraler Stelle aus und nutzt die kombinierte Leistung, um weitere Schadsoftware zu verbreiten oder DDoS-Angriffe (siehe dort) zu starten.

**DDoS**
Denial-of-Service-Angriffe richten sich gegen die Verfügbarkeit von Diensten. Ziel ist es, Websites, einzelne Systeme oder ganze Netzwerke durch unzählige gleichzeitige Anfragen lahmzulegen.

**Exploit**
Ein Exploit ist die Möglichkeit, Schwachstellen auszunutzen, die bei der Entwicklung von Hard- und Software entstanden sind. Dabei werden Sicherheitslücken und Fehlfunktionen von Programmen oder Geräten verwendet, um sich Zugang zu verschaffen. Eine spezielle Form ist der Drive-by-Exploit: Hier werden, etwa schon beim bloßen Betrachten einer Website, automatisiert Schwachstellen im Browser oder im Betriebssystem ausgenutzt, um Schadsoftware zu installieren.

**Malware**
Ein anderer Begriff für Schadsoftware oder Schadcode; das Kunstwort ist abgeleitet aus Malicious Software und bezeichnet Software, etwa Trojaner und Viren, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Schadsoftware ist üblicherweise für ein bestimmtes Betriebssystem, etwa Windows oder Android, konzipiert.

**Phishing**
Zusammensetzung aus »Password« und »Fishing«: Die Angreifer versuchen, über gefälschte Websites, E-Mails oder Whatsapp-Nachrichten an persönliche Daten eines Internetnutzers zu gelangen, zum Beispiel Log-in-Daten oder Kreditkarteninformationen. Diese werden dann verwendet, um in weitere Systeme einzudringen, oder weiterverkauft.

**Ransomware**
Schadprogramme, die es dem Opfer unmöglich machen, auf die eigenen Daten oder Systeme zuzugreifen, indem sie die Inhalte verschlüsseln. Erst gegen Zahlung eines Lösegelds, meist in Form von Kryptowährungen, heben die Erpresser die Sperre wieder auf – wenn man Glück hat.

**Supply-Chain-Angriff**
Hier werden Backdoors (siehe dort) und Malware (siehe dort) nicht direkt in ein System eingeschleust, sondern über Software von Dritten. Es werden gezielt Schwachstellen bei Softwareentwicklern und Dienstleistern gesucht, um über deren Produkte auf die Systeme der Kunden zu gelangen.

IT-Sicherheitsexperte und einer der Sprecher der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS). Vor allem kleine und mittlere Unternehmen, Organisationen und Kommunen seien häufig unzureichend aufgestellt, wenn es um die Abwehr von Cyberangriffen geht.

Die Gründe sind vielfältig. Eine Erklärung ist, dass sich Art und Weise der Angriffe verändern. Lange Zeit haben sich die Opfer vor allem Schadsoftware eingefangen, weil Mitarbeiter verseuchte Websites und Dateien aufriefen. Viren, Trojaner und Computerwürmer wurden von den Angreifern mit Hilfe von Botnetzen (siehe Glossar) möglichst breit gestreut, um möglichst viel unkoordinierten Schaden anzurichten. »Diese Art von Schwachstellen hat man mittlerweile einigermaßen gut unter Kontrolle«, sagt Thorsten Holz, Professor am Lehrstuhl für Systemsicherheit an der Ruhr-Universität Bochum. »Die Angreifer sind professioneller geworden, es gibt weniger Einzelkämpfer und stattdessen mehr organisierte Gruppen, die Hacking als Dienstleistung anbieten«, sagt Holz.

Das führt dazu, dass die Ziele immer genauer ausgewählt werden. Vor allem bei Ransomware-Attacken wollen die Angreifer möglichst zahlungskräftige Opfer finden; sie haben es darum meist auf Unternehmen oder die Betreiber kritischer Infrastruktur abgesehen. Beim Angriff auf die US-amerikanische Colonial Pipeline im Mai konnten damit rund 3,6 Millionen Euro erbeutet werden. »Statt sofort anzufangen, alles zu verschlüsseln, meldet der Schadcode dem Angreifer häufig erst einmal, dass er ein System infiltriert hat«, sagt Michael Wiesner. »Dann schauen die Hacker, wen sie eigentlich vor sich haben und was dort zu holen ist, teilweise werden sogar zunächst Firmenbilanzen überprüft.«

Um Schadcode einzuschleusen, nutzen die Kriminellen zunehmend so genannte Supply-Chain-Angriffe aus. So geschehen etwa im Fall von SolarWinds oder beim Hack des US-Dienstleisters Kaseya: In beiden Fällen infiltrierten die Hacker zunächst die Hersteller von Spezialsoftware, die die Opferfirmen nutzen. Auf dem Rücken dieser Systeme drangen sie dann in die IT der Kunden vor. Das Perfide: Firmen müssen der Software, die sie von

»Ich kann mich nicht gegen alle Angriffe verteidigen. Früher oder später wird irgendetwas durchkommen.«
(Richard Werner, IT-Sicherheitsunternehmen Trend Micro)