


# die WIRTSCHAFT

03 | 2023

Ausgabe:  
IHK Ulm

zwischen Alb und Bodensee

**6 Initiative Wirtschaft 4.0**Zehn-Punkte-Zukunfts-  
Programm beschlossen**56 Bildungsmesse 2023**Ein Erfolg für Aussteller,  
Veranstalter und Besucher**78 Factoring**Liquidität sichern,  
Kosten im Blick behalten**Chefsache  
Cybersicherheit**So bereiten Sie Ihr Unternehmen  
auf den Ernstfall vor**22**

A portrait of Tobias Eggendorfer, a man with short brown hair and a slight smile, wearing a blue zip-up hoodie. He is looking slightly to the right of the camera. The background is a plain, light-colored wall.

Tobias Eggendorfer,  
Professor für IT-Sicherheit  
an der Hochschule Ravens-  
burg-Weingarten, legt  
Unternehmen nahe, sich  
bei wichtigen Sicherheits-  
fragen mit erfahrenen  
IT-Spezialisten aus-  
zutauschen.

# Cyber- und Informationssicherheit

Cyberkriminalität ist allgegenwärtig: Allein im Jahr 2021 hat das Bundeskriminalamt 146.363 Fälle erfasst. Davon konnten weniger als 30 Prozent aufgeklärt werden. Bei einer Umfrage des deutschen Digitalverbands Bitkom vom September 2022 gaben 84 Prozent der befragten 1.000 Unternehmen an, in den letzten zwölf Monaten Cyberattacken erlebt zu haben. Experten erwarten einen weiteren Anstieg, ermöglicht durch neue Technologien wie Chatbots. Die Größe oder Branche eines Unternehmens spielt bei einem Angriff kaum eine Rolle. Betroffen sind KMUs, Großkonzerne, Startups und öffentliche Einrichtungen gleichermaßen. Doch wie können sich Unternehmen schützen? Wir haben mit Experten gesprochen. Auch Betroffene kommen zu Wort und berichten von ihren eigenen Erfahrungen nach einer Cyberattacke.


**IN KÜRZE**
**Leitfaden für IT-Sicherheit in Unternehmen**

Wo liegen die Risiken im Bereich IT-Sicherheit, was kann ein Unternehmen tun, um sich vor Cyber-Angriffen zu schützen? An wen kann ich mich bei Fragen wenden, wer hilft mir, mein Unternehmen für den Ernstfall fit zu machen? Antworten auf diese und viele weitere wichtige Fragen finden Sie im Leitfaden unter dem folgenden Link:

[www.ihk.de/bodensee-oberschwaben](http://www.ihk.de/bodensee-oberschwaben),  
Dokument-Nr. 1941832

**Hilfsangebot:  
Sec-O-Mat**

Die Transferstelle IT-Sicherheit im Mittelstand (IT-SiM) – das neue Förderprojekt des Bundesministeriums für Wirtschaft und Energie – bietet kleinen und mittelständischen Unternehmen kostenfreie Angebote und Werkzeuge zur Unterstützung im Bereich IT-Sicherheit. Darunter auch den Sec-O-Mat, eine Webanwendung, die Unternehmer mithilfe eines Fragebogens zu ihren IT-Sicherheitsanforderungen durch den Prozess bis hin zum Aktionsplan begleitet.

[www.ihk.de/ulm](http://www.ihk.de/ulm),  
Dokument-Nr. 5449424

Bild: Fotostudio/arsmedia


**Dominik Schwärzel ist CEO der Wilken Software Group in Ulm und hatte erst kürzlich im eigenen Unternehmen mit einem Cyberangriff zu kämpfen.**

**E**s geschah in der Nacht des 12. Oktober 2022. Bei der Wilken Software Group aus Ulm fielen trotz umfassendem Notfallkonzept im Minutentakt immer mehr Dienste aus. Am nächsten Morgen stand fest: Über einen Verschlüsselungstrojaner wurde eine Cyberattacke auf das IT-Unternehmen gestartet. „Wir hatten keinen Zugriff mehr auf bestimmte Anwendungen“, erinnert sich CEO Dominik Schwärzel. Nun war schnelles Handeln gefragt. Sprich: Server und Netzwerke entkoppeln, ganze Systeme herunterfahren. „Zum Glück wa-

ren aufgrund physikalisch getrennter Netzwerke unsere Kundendaten zu jeder Zeit geschützt. Das hat uns erstmal durchatmen lassen“, so Schwärzel. Eine lohnenswerte Vorsichtsmaßnahme. Denn in vielen Fällen haben es Hacker auf diese sensiblen Daten abgesehen, um sie weiterzuverkaufen oder zu Erpressungszwecken zu benutzen.

**Best Practice für Worst-Case-Szenario**

Als ISO-zertifiziertes Rechenzentrum verfügt Wilken über einen durchdachten Notfallplan. Diese Vorbereitung machte sich nun bezahlt. Als nächstes wurde ein Krisenstab ins Leben gerufen. „Durch Corona waren wir zum Glück geübt darin“, schmunzelt Schwärzel. Dabei wurden Teilprojekte festgelegt und entsprechend priorisiert. An erster Stelle stand für die Wilken Group die Kommunikation. Das Unternehmen war zu diesem Zeitpunkt weder über Telefon noch via Internet oder E-Mail zu erreichen. Also wurden vie-

le Kunden direkt angerufen und Informationen über die Presse verbreitet, um Transparenz zu schaffen. Weil Wilken das Intranet auf einen separaten Cloud-Anbieter ausgelagert hatte, konnten die Mitarbeiter schnell über die nächsten Schritte gebriefet werden. Ein Effekt überraschte den Geschäftsführer besonders: „Wir entwickelten eine ungeheure Kraft. Wenn man von außen angegriffen wird, schweißt das unglaublich zusammen.“ In den ersten Tagen erfolgte eine Umstellung auf Schichtdienst. Es wurde sogar Nachts gearbeitet, um alles schnell wieder zum Laufen zu

bringen. Dennoch seien die ersten Tage ein Blindflug gewesen, erinnert sich der Wilken-CEO. „Wir waren dabei, neue Systeme aufzubauen, den Angriffsvektor zu bestimmen und wussten noch nicht, mit welchen Aus-

wirkungen auf andere interne Systemgebungen wir noch zu rechnen hatten.“ Zeitgleich lief im Hintergrund die IT-Forensik.

Durch die Entkopplung der Kundendaten sowie die Auslagerung des Intranets auf externe Cloud-Server, aber vor allem durch ein gut strukturiertes Krisenmanagement konnte das 600 Mitarbeiter starke Unternehmen nach nur einer Woche wieder ans Netz gehen. Nach weiteren acht Wochen war es wieder vollständig arbeitsfähig. Ein erstaunlich kurzer Zeitraum für einen Angriff dieser Größe. „Wir sind nicht nur mit einem blauen Auge davongekommen, sondern sogar gestärkt daraus hervorgegangen“, zieht Schwärzel ein Resümee. Erstens konnte die Wilken Group

“  
„Wir sind gestärkt daraus hervorgegangen.“  
“

Dominik Schwärzel, CEO der Wilken Software Group, Ulm

den Cyberangriff dazu nutzen, Strukturen neu aufzubauen, zu optimieren und bestehende Systeme zu hinterfragen. Unterm Strich ein großer Effizienzgewinn. Zweitens: „Wir erhielten viele Neukundenanfragen auch aus der Region, die in unser Rechenzentrum wollten. Sie waren beeindruckt, wie gut wir die Cyberattacke gemeistert hatten.“ Fazit: Wilken hat als Best-Practice-Beispiel für den Worst Case positive Aufmerksamkeit erregt.

### Unternehmen kaum auf Ernstfall vorbereitet

Der Wilken-Fall zeigt noch etwas: „Egal, wie professionell und IT-affin ein Unternehmen aufgestellt ist, es kann jeden treffen“, so Schwärzel. Diese Erfahrung kann auch Martin Theimer, Vertriebsleiter bei der SOFT-CONSULT Häge GmbH in Langenau, nur bestätigen. Er bemängelt die fehlende Wahrnehmung für das Thema Cybersicherheit. So ergab eine Umfrage des Gesamtverbands der Deutschen Versicherungsgesellschaft (GDV), dass 48 Prozent aller Unternehmen keinen Notfallplan oder IT-Dienstleister für den Ernstfall haben. „Es gibt kaum einen Produktionsprozess, der heute nicht EDV-gesteuert ist“, sagt Theimer. „Daher sind zwei von drei Firmen nach einem Angriff stark bis sehr stark eingeschränkt.“ Außerdem rechnet er mit einer Zunahme von Ransomware-Attacken. Laut dem Bundeskriminalamt lagen die durch Ransomware verursachten Schäden im Jahr 2021 in Deutschland bei 24,3 Milliarden Euro. Solche Attacken ließen sich sehr leicht starten und könnten heute im Darknet als Paket gebucht werden. „Verschlüsselungsattacken via E-Mail sind mittlerweile viel besser geworden und zum Beispiel in fehlerfreiem Deutsch geschrieben“, so Theimer. Unternehmen rät er, ein Meldesystem bei Verdachtsfällen einzurichten. Dies funktioniere aber nur, wenn es positiv in der Unternehmenskultur verankert werde: „Statt den Mitarbeiter zu tadeln, dass er womöglich auf eine Phishing-E-Mail geklickt hat, sollten Sie ihn für die offene Kommunikation loben. Sprich: Toll, dass du dich meldest, wir schauen uns den Vorgang an.“

### Sicherheitslösungen – am besten mehrgleisig fahren

Ein wichtiges Schlagwort in punkto Cybersicherheit sieht Martin Theimer in einem guten Patch-Management. Für den Mittelstand seien regelmäßige Security-Checks sehr wichtig. Doch es sei sehr aufwändig, sich bei der Vielzahl der Programme auf dem neuesten Stand zu halten. Und nicht jede Firma könne sich einen eigenen IT-Experten leisten. „Es gibt hierfür nicht genügend Fachkräfte“, sagt Theimer. So sei es für viele Firmen praktikabler, das Patch-Management an IT-Dienstleister auszulagern. Security-Checks sollten laut dem Experten mindestens alle drei Monate durchgeführt und Updates monatlich geprüft werden. Die SOFT-CONSULT Häge GmbH prüft im Zuge ihrer Servicepakete sogar wöchentlich. Auch Mitarbeiterschulungen sollten mindestens einmal pro Jahr auf dem Programm stehen, so Theimer: „Cybersicherungen fordern all diese Punkte. Kommt es zu Versäumnissen, wird Ihre Police unwirksam und Sie stehen ohne finanzielle Absicherung da.“

Ein weiterer Tipp von dem IT-Fachmann: „Schaffen Sie verschiedene Brandschutzzonen. Bricht irgendwo Feuer durch einen Angriff aus, kann es sich nicht so leicht auf andere Bereiche ausweiten.“ Dazu gebe es viele Möglichkeiten: Trennung von Nutzer- und Administratorkonten, Sperrung der USB-Ports für Datenträger, Einloggen ausschließlich über eine VPN-gesicherte Leitung sowie eine Multifaktor-Authentifizierung. Ein Backup-Management zur Sicherung der Daten sei ebenso wichtig, sagt Theimer: „Fragen Sie sich, welche Systeme Sie auf Ihren eigenen Servern belassen und welche

 **SOFT-CONSULT**

Ihr Partner für  
IT-Security  
im Mittelstand.



Schützen Sie wirksam die Informationen, Prozesse, Systeme und Netzwerke in Ihrem Unternehmen – mit einer individuellen Beratung und maßgeschneiderten Security-Maßnahmenpaketen.

#### Unser Portfolio:

- IT-Sicherheits-Check:
  1. Bestandsaufnahme
  2. Schwachstellen-Scan
  3. Präsentation der Ergebnisse
  4. Behebung von erkannten Schwachstellen
- Managed Security Services wie z. B. Managed Firewall oder Managed Backup
- IT-Awareness-Training

SOFT-CONSULT Häge GmbH

Riedheimerstraße 5  
89129 Langenau

Tel. 07345 9611-0  
sc@soft-consult.net  
www.soft-consult.net



Martin Theimer, SOFT-CONSULT Häge GmbH, Langenau, rät Unternehmen dazu, ein Meldesystem einzurichten, um bei Verdachtsfällen einschreiten zu können.

Sie auf eine Cloud auslagern wollen. Letzteres spart Ressourcen für Wartung und Personal.“

### Cyberdefence kann Leben retten

Tobias Eggendorfer ist Professor für IT-Sicherheit an der Hochschule Ravensburg-Weingarten. Momentan hat er sich beurlauben lassen, um die Leitung der Abteilung „Sichere Systeme“ bei der Agentur für Innovation und Cybersicherheit (Cyberagentur) zu übernehmen. „Die Cyberagentur vergibt Forschungsaufträge im Bereich Cybersicherheit zu Themen, bei denen der Erfolg noch ungewiss ist, die aber in fünf bis zehn Jahren relevant sein werden“, erläutert Eggendorfer. Verschlüsselungstechnologien, cyberresiliente Gesellschaft, Bionik, Quantentechnologie, Robotik, Schutz der Infrastruktur bis in die maritime Tiefsee hinein – solche Themenfelder lägen im Fokus. Cyberdefence könne lebensrettend sein: „Ob Herzschrittmacher, Insulinpumpen oder Geräte auf der Intensivstation – sie alle haben digitale Schnittstellen“, sagt Eggendorfer. Diese könnten theoretisch von außen gehackt werden. Erste Krisis handelten diese Methoden bereits literarisch ab. Auch Smart Devices wie digital gesteuerte Heizsysteme oder autonomes Fahren zeigten, wie wichtig Cybersicherheit schon heute ist.

### Penetrationstest und Qualitätskontrolle

Umso mehr ärgert sich Eggendorfer über die marode IT-Landschaft weltweit. Dafür sieht er mehrere Gründe: „Wir haben Systeme, die per se anfällig sind und deren Sicherheitslücken schon seit Jahrzehnten bestehen.“ Auch das BGH-Urteil von 1986, das oft dahingehend fehlinterpretiert werde, dass Software

nicht fehlerfrei sein könne, sei wenig hilfreich gewesen. Denn Eggendorfer ist der Überzeugung, dass es sichere Systeme gibt. Diese hätten sich nur kaum auf dem Markt durchsetzen können und seien von Monopolisten wie Microsoft verdrängt worden. Weiterer Punkt: „Bei Software haben Sie keine Qualitätserwartungen. Sie können die immaterielle Qualität nur oberflächlich prüfen und nicht anfassen wie ein Möbelstück.“ Also gäben sich viele Unternehmen mit fehlerhaften Systemen zufrieden und packten einfach Malwarescanner und Firewalls obendrauf. Für Eggendorfer keine Dauerlösung: „Wenn Ihr Auto alle fünf Kilometer stehen bleibt und nach einem neuen Update verlangt, würden Sie diesen Zustand auch nicht hinnehmen.“

Der Professor für IT-Sicherheit rät jedem Unternehmen vor dem Kauf eines Softwaresystems, dieses genau prüfen zu lassen: „Fordern Sie einen vollständigen Penetrationstest ein

“

„Schaffen Sie verschiedene Brandschutzzonen.“

Martin Theimer, SOFT-CONSULT Häge GmbH, Langenau

“

und nicht nur ein oberflächliches Buzzword-Bingo.“ Ein Penetrationstest entspreche dem Pendant zum Auto-TÜV.

Auch an der kulturellen Problematik müsse angesetzt werden: „Länder wie Estland haben bereits komplett auf E-Government umgestellt, weil dort alle an einem Strang ziehen.“ Hierzulande gebe es Vorbehalte wegen vieler missglückter IT-Projekte, zum Beispiel das beA-Anwaltspostfach der Bundesrechtsanwaltskammer oder der elektronische Personalausweis. Dazu kämen fragliche Qualifikationen in Schlüsselpositionen wie die der Datenschutzbeauftragten, die laut Eggendorfer „ein Zertifikat erhalten, wenn sie einen zweitägigen Kurs absolvieren. Egal, welchen Beruf sie vorher ausgeübt haben. Es gibt keinerlei Zugangsvoraussetzungen.“ Darunter leide häufig die Qualität. Eggendorfer legt Unternehmen nahe, sich bei wichtigen Sicherheitsfragen mit erfahrenen IT-Spezialisten auszutauschen, die über ein entsprechendes Studium und Erfahrung mit verschiedenen Systemen verfügen.

### Sind Narzissten besonders anfällig?

Mit der menschlichen Seite von Cyberkriminalität befasst sich Stefan Sütterlin. Er ist Professor an der Hochschule Albstadt-Sigmaringen im Fachbereich Informations- und IT-Security sowie Cyberpsychologie. „Laut aller verfügbaren polizeilichen Statistiken ist das Ausnutzen menschlicher Schwächen Bestandteil fast jeder Cyberattacke“, zitiert Sütterlin. Dabei gehe es stets um die Frage, wie man an die Daten von Personen gelangen, sich Zugang zu deren Systeme verschaffen oder sie zu Handlungen wie Geldüberweisungen bewegen kann. Die Angriffsvektoren änderten sich mit der technischen Entwicklung: „Dem Einzeltrick am Telefon entsprechend, sind es hier Deepfakes, Phishing-Mails oder der absichtlich platzierte USB-Stick.“

Attacken wie individualisiertes Spear Phishing oder Whaling – welches sich gezielt gegen Führungskräfte oder Entscheider richtet – beruhen auf Social Engineering. „Inzwischen ist es möglich, mithilfe von Computerprogrammen Persönlichkeitsprofile anhand von Social-Media-Accounts zu erstellen. Sie nutzen die jeweiligen Vorlieben oder Schwächen als Einfallstor aus“, so Sütterlin. Es werde Vertrauen aufgebaut und Neugierde geweckt. Diese Art von Mails wirken glaubwürdiger, weil sie als Absender den Namen von Kunden, Vorgesetzten oder Institutionen tragen. Entsprechende Informationen würden vorab recherchiert und auf den jeweiligen Persönlichkeitstyp zugeschnitten. Ein einfaches hypothetisches Beispiel: Computerprogramme erfassen, wie oft eine Person auf Fotos

# „Mitarbeiter sind nicht das schwächste Glied, sondern die letzte Hoffnung im Bereich Cyberdefence.“

Stefan Sütterlin, Hochschule Albstadt-Sigmaringen

auftaucht, was sie liked, kommentiert, wem sie folgt. „Extrovertierte Menschen posten viele Fotos, aber auch Landschaftsaufnahmen, sagt Sütterlin. Der Persönlichkeitstyp des Narzissen postet hingegen fast nur Selfies von sich selbst.“ Spear-Phishing-Mails könnten nun folgendermaßen lauten: „Sie wurden auf einem Foto von Veranstaltung XY markiert.“ Handelt es sich um Akademiker: „Ihr Beitrag wurde kommentiert.“ Oder: „Einladung zur Expertenrunde“. Stimmen Anlass und Absender, klicken viele auf den entsprechenden Link. Bei anderen Persönlichkeitstypen werde beispielsweise auf Hilfsbereitschaft abgezielt oder ein Zeitdruck-Szenario aufgebaut.

## Schwer zu durchschauen: Spear Phishing & Deepfakes

Um sich vor Spear Phishing zu schützen, empfiehlt der Cyberpsychologe individuelle Mitarbeiterschulungen, da jeder Mensch eigene Einfallstore habe. Dazu gebe es bereits gut aufbereitete wissenschaftliche Fragebögen und Methoden. Diese führen dazu, dass ein höherer Grad der weitgehend automatisiert gesteuerten Individualisierung effizienter und zeitsparender sein kann. Individualisiertes Training bedeutet also nicht mehr, sondern weniger Aufwand, bei besseren Resultaten. Bei standardisierten Schulungen bemängelt Sütterlin die schlechte Qualitätskontrolle: „Laut Studien reduziert sich die Chance, dass jemand auf solche Tricks hereinfällt, nach der Schulung um 20 bis 80 Prozent. An dieser Spanne erkennen wir sowohl das Potenzial als auch das Risiko, es falsch anzugehen.“ Bei manchen Firmen hätte die Schulung langfristig so gut wie nichts gebracht. Awareness, Intention, Han-

deln und Gewohnheit – das sind für Sütterlin die vier Schritte, die zu einem nachhaltigen Erfolg führen. Auch IT-Fachkräfte seien durch Selbstüberschätzung nicht vor Fehlern gefeit. Eine gemeinsam mit norwegischen Forschern durchgeführte Studie der Hochschule Albstadt-Sigmaringen legte 300 Personen zehn Videos mit Aussagen von Personen vor. Teils Originale, teils Deepfakes. Die Probanden sollten sich einschätzen, wie gut sie echte von gefälschten Videos unterscheiden können. Das Ergebnis ließ aufhorchen: „Normale Mitarbeiter hatten sich im Durchschnitt um 20 Prozent überschätzt, IT-Fachkräfte aber um 80 Prozent. Frauen lagen in ihrer Einschätzung mit Faktor 1,0 genau richtig“, so Sütterlin. Menschen, die zur Selbstüberschätzung neigen, seien auch im Falle größeren Fachwissens ein potenzielles Sicherheitsrisiko. Ebenfalls nicht zu vernachlässigen sei der interne Daten- und Informationsdiebstahl durch Mitarbeiter. Rache sei hier das zentrale Motiv, wie im Fall einer Kündigung. All diese Beispiele zeigten: „Wenn Menschen andere Menschen über einen technischen Weg angreifen, kann man sich nicht nur auf die Technik in der Mitte konzentrieren, wenn am Anfang und Ende immer noch der Mensch steht.“ Vieles sei auf dieser Ebene bereits machbar,

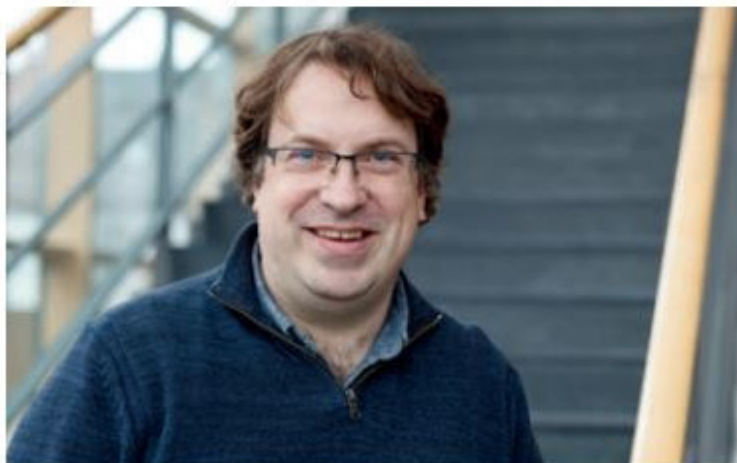
wenn das Bewusstsein vorhanden ist, betont Sütterlin. Doch der Gedanke, man sei als Unternehmen zu klein oder nicht systemrelevant, sei weit verbreitet. Es gebe keine uninteressanten Informationen: „Alles, was die Existenz Ihrer Firma sichert, ist für Cyberkriminelle von Interesse.“

## Was Experten wünschen und raten

Martin Theimer wäre glücklich, wenn sich das Notfallmanagement von Unternehmen mehr in Richtung Vorsorge verlagern würde: „IT-Dienstleister sind nicht nur dazu da, um bei Problemen kontaktiert zu werden. Sie stehen für den regelmäßigen Austausch zur Verfügung.“ Dominik Schwärzel legt allen Firmen nahe, schnell eine Cyberversicherung abzuschließen, falls sie noch keine haben: „Die Policen erhöhen sich momentan um mehrere Hundert Prozent. In zwei Jahren werden sie vermutlich gar keine vernünftig abgesicherte Police mehr bekommen.“ Zudem sollten Firmen einen Notfallplan ausarbeiten, damit am Tag X jeder Mitarbeiter seine klaren Aufgaben und seine Rolle kennt. Tobias Eggendorfer empfiehlt, die Abhängigkeit von bestehenden Betriebssystem-Anbietern zu reduzieren. Er glaubt daran, dass sich in Zukunft die besten und nicht die werbewirksamsten Produkte durchsetzen werden. Ein weiterer Tipp von ihm: „Die Landesämter für Verfassungsschutz können Sie präventiv bei Spionagegefahr sowie nach einem Hackerangriff beraten.“

Stefan Sütterlin hofft auf eine bessere interdisziplinäre Vernetzung: „Es gibt momentan noch keinen Studiengang, der bei der IT-Sicherheit Bereiche wie Recht, Risikomanagement, Ethik und Psychologie gänzlich einbezieht. Auch wenn wir dem Ganzen an unserer Hochschule schon recht nahekommen.“ Zudem wünscht er sich ein Umdenken: „Mitarbeiter sind nicht das schwächste Glied, sondern die letzte Hoffnung im Bereich Cyberdefence. Man sollte sich seiner Selbstwirksamkeit im positiven Sinne bewusst sein.“

Diana Wieser,  
Inhaberin von adWORDising  
Journalismus & Werbetext, Ulm



Stefan Sütterlin, Professor an der Hochschule Albstadt-Sigmaringen, weiß: Bei fast jeder Cyberattacke werden menschliche Schwächen ausgenutzt.