MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE MÄRZ 2022
CYBER-WAR UND CYBER-TERRORISMUS

TECHNOLOGIE KANN KRIEGE ENTSCHEIDEN

Auf dem Schlachtfeld diktieren hochgradig technologisierte Kampfsysteme. Doch selbst unter der Kriegsschwelle spielt Technologie eine elementare Rolle, wie unser Beitrag illustriert.

DIE GEFAHR VON CYBER-TERRORSMUS

Terroristische Angriffe im Cyberraum können eine technologisierte Gesellschaft empfindlich treffen. Den Risiken muss man sich bewusst sein und diese konkret adressieren.

März 2022: Nachschub ist wichtig

Der Einmarsch der russischen Streitkräfte in die Ukraine wird in vielerlei Hinsicht in die Geschichte eingehen. Unter anderem auch als *Vorzeigebeispiel* dessen, dass eine der wichtigsten Grundsätze sträflichst missachtet wurde: Gewährleisten von zeitnahem und konsequentem *Nachschub*.

Viele Fahrzeuge, vor allem die T-Panzer aus der Zeit der Sovjetunion, konnten nicht mehr mit Diesel befüllt werden. Dadurch kamen sie zum Erliegen und wurden damit weitestgehend kampfunfähig, ohne jemals Feindkontakt gehabt zu haben.

Nachschub ist aber auch im IT-Bereich wichtig: Ausbildung neuen Personals, Anschaffen und Austauschen von Hardware, Gewährleisten von Ausfallsicherheit, Warten von Systemen sowie Aktualisieren von Software und Einspielen von Patches.

Nicht selten herrscht grosse Euphorie, wenn ein neues Produkt angeschafft oder ein neuer Server installiert wird. Doch gerne vergisst man eben die Verpflichtungen, die damit einhergehen. Der Nutzen einer Lösung ist massgeblich davon abhängig, wie sie betrieben und bewirtschaftet werden kann. Dies darf in aller Euphorie nicht vergessen werden.

Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

INTERVIEW ZU MILITÄRISCHEN CYBERANGRIFFEN AUF UKRAINE

Im Zuge des Einmarsches *russischer Truppen in die Ukraine* wird verschiedenenorts besprochen, welche Rolle vorgängig und gegenwärtig Cyberangriffe spielen. Marc Ruef ist Korrespondent und Kolumnist der *Allgemeinen Schweizerische Militärzeitschrift* (ASMZ). Im Interview mit dem Journalisten Tobias Bolzern erklärt er, welche Möglichkeiten gegeben sind und wie diese angestrebt werden.

INTERVIEW ZU SMS-ANGRIFF WÄHREND ABSTIMMUNG

Der Podcast *Hotspot* auf SRF widmet sich in der aktuellen Folge dem Thema *Dark Social*. Im ersten Teil wird diskutiert, welchen Einfluss die massenweise verschickten SMS auf die *Abstimmung zum Covid-Gesetz* hatte. Der Journalist Julian Schmidli hat Marc Ruef befragt, woher die gesammelten Telefonnummern stammen, wie solche Aktionen zu werten sind und welche gesellschaftlichen Auswirkungen sie haben können.

FERNSEHINTERVIEW ZUM ABHÖREN DURCH SMARTPHONES

In der Sendung *10vor10 auf SRF* wurde unter anderem der Mythos diskutiert, ob uns *Smartphones ständig abhören*, um personalisierte Werbung generieren zu können. Hierfür haben sich die Journalisten Pirmin Roos und Mirjam Spreiter mit Marc Ruef unterhalten. Im Interview zeigt er auf, mit welchen technischen Hilfsmitteln sich Smartphones auf eine solch versteckte Funktion hin untersuchen lassen.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 11ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-26-7) als auch in englischer Sprache (ISBN 978-3-907109-27-4) verfügbar. Das Vorwort wurde von Marko Rogge, seines Zeichens IT-Sicherheitsbeauftragter für Mobile Security bei der Deutschen Bahn AG, verfasst.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen und Bestellungen auf unserer Webseite.

ISBN 978-3-907109-26-7 [de]
ISBN 978-3-907109-27-4 [en]

NACHHALTIGKEIT ERMÖGLICHT SICHERHEIT

Bildquelle: https://pixabay.com/image/id-7039471/

MARC RUEF

WIE TECHNOLOGIE EINEN KRIEG ENTSCHEIDEN KANN

Vor über 10 Jahren hatte ich die Möglichkeit das Thema Cyber im Rahmen der Armeeführung zu diskutieren. Bei diesem Gespräch wurde von verschiedenen Seiten geäussert, dass *Cyber keinen Krieg entscheiden würde*. Das war damals falsch und ist es heute umso mehr. Ein unnötiger Denkfehler, den man im Informationszeitalter tunlichst vermeiden sollte.

Wir leben in einer Ära, in der unsere Existenz durch *Elektronik*, *Digitalisierung* und *Informationsverarbeitung* zusammengehalten, das Zusammensein orchestriert und Lebensqualität gewährleistet wird. Cyber hat aber nicht nur mit Bits und Bytes zu tun. Im Rahmen von Sicherheitsüberprüfungen wird gerne das Augenmerk auf technisch versierte Hacking-Angriffe gelegt, obschon viele Firmen ihre Zuleitungen und Sicherungskästen für Strom ungeschützt und frei zugänglich umgesetzt haben.

Strom ist nur eines der Elemente, das zur *kritischen Infrastruktur* gehört. Wenn dieser Ausfällt, ist nach Stunden mit Chaos und nach Tagen mit Plünderungen zu rechnen. Denn mit ihm werden ebenso die Wasserversorgung, Kommunikation und der Verkehr zusammenbrechen.

Die Gewinnung und Verteilung von Strom wird wiederum durch moderne *Computer- und Netzwerktechnologien* ermöglicht. Ein elektronischer Angriff auf zentrale Elemente kann somit über kurz oder lang eine Gesellschaft empfindlich treffen. Szenarien, die sowohl unter als auch über der Kriegsschwelle dank der gesellschaftlichen digitalen Transformation an Relevanz gewonnen haben.

GEOPOLITISCHE INTERESSEN

Computerangriffe sind in einer global vernetzten Welt an der Tagesordnung. Manche von ihnen werden durch *Cyberkriminelle* vorangetrieben, die mit Diebstahl und Erpressung ihren Lebensstil finanzieren wollen. Andere werden durch *staatliche Akteure* orchestriert, um ihre geopolitischen Interessen durchsetzen zu können. Der Unterschied in Bezug auf Herangehensweise und involvierte Figuren ist manchmal fliessend, die klare Identifikation und Assoziation der Akteure umso schwieriger.

Es bestehen aber Möglichkeiten, diese Aktivitäten, oder mindestens die Resultate dieser, zu beobachten. Dadurch können sowohl für einzelne Akteure als auch für Gruppierungen entsprechende *Profile* er-

stellt werden: Welche Technologien sind relevant und welche Produkte als Ziel ausgewählt. Setzt man dies in Kontext mit den wirtschaftlichen bzw. geopolitischen Absichten, lassen sich bisweilen ziemlich genaue Voraussagen in Bezug auf geplante, sich anbahnende oder laufende Aktivitäten erstellen.

Zum Beispiel ist ersichtlich, dass man in China vor rund 2 Jahren den strategischen Entscheid gefällt hat, ebenfalls Angriffsszenarien anzustreben, die eine *Benutzerinteraktivität* voraussetzen können. Dazu gehören klassische Phishing- und Social Engineering-Szenarien, in denen die Zielperson zu einer kompromittierenden Handlung gedrängt wird. Dies kann typischerweise die Herausgabe von Passwörtern oder das Installieren einer Malware sein.

Diese Stossrichtung steht in grossem Widerspruch zu den Paradigmen, die man zum Beispiel bei US-amerikanischen, russischen oder israelischen Akteuren beobachten kann. Dort werden primär rein technische Angriffsmöglichkeiten bevorzugt, bei denen der wankelmütige Faktor Mensch keine Rolle spielt. Diese Methoden sind technisch aufwändiger fehlerfrei umzusetzen, lassen sich aber ebenso schwierig frühzeitig erkennen und in Echtzeit abwehren.

Solche Details, gerade wenn sich aus diesen eine solide Prognose ableiten lassen, sind von enormer Wichtigkeit. Sie helfen dabei, selbst strategische und taktische Entscheidungen zu treffen, um Angriffe frühzeitig identifizieren und diese erfolgreich mitigieren zu können. Im Idealfall kann man proaktiv gegen die drohenden Gefahren vorgehen, oder halt mindestens souverän reagieren.

OFFENSIVE ANFORDERUNGEN

Doch auch auf offensiver Seite hat eine Professionalisierung und Industrialisierung stattgefunden. Das Umsetzen von technischen Angriffen wird mit sogenannten *Exploits* automatisiert. Das Entwickeln dieser wurde über die Jahrzehnte immer schwieriger, da Computersysteme fortwährend komplexer und Abwehrmechanismen zunehmend ausgeklügelter wurden. So ist es nicht erstaunlich, dass sich ein *Markt für diese Exploits* etablieren konnte: Dort werden Angriffstools getauscht, verkauft und gekauft.

Analysen dieser Märkte zeigen Trends in Bezug auf beliebte Angriffsziele und Preisentwicklungen auf. Als Faustregel gilt, dass umso populärer ein Produkt aus Sicht der Angreifer ist, desto höher sind die Prei-

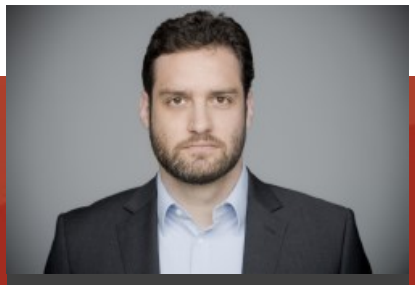
se. Exploits für iPhones führen seit Jahren die Rangliste an, erzielen regelmässig Preise über 1.5 Millionen USD. Dies liegt einerseits an der Architektur des Apple-Betriebssystems. Andererseits an den potenziellen VIP-Zielen, die mit einem guten Exploit angegangen werden können.

Am Schluss gewinnt derjenige mit dem besten Wissen. Durch den Zukauf von Exploits muss dieses in grossen Teilen nicht mal selbst erarbeitet werden. Es bleibt in diesem Moment eine Frage des Geldes. Wer im internationalen Spiel im Cyberraum mithalten will, muss sich also nicht nur defensiv, sondern auch offensiv richtig aufstellen können. Entsprechendes Budget wird mittlerweile bei den dafür zuständigen Organisationen vorgesehen. Und das Mindset kann sich langsam auch mit der digitalen Transformation anfreunden.

FAZIT

Unsere Gesellschaft fusst auf den neuen Technologien. Durch sie erhalten wir Wohlstand und Lebensqualität. Gleichzeitig sind sie aber auch ein *faustischer Pakt mit dem Teufel*. In vielen Bereichen tendieren sie uns zu beherrschen. Dem kann nur mit klugen Entscheidungen und organischem Wachstum entgegnet werden. Primitiv anmutende Grundwerte wie Unabhängigkeit und Simplizität sind unabdingbar, um von der Technologie nicht überrollt zu werden.

Die Digitalisierung hat auch vor militärischem Equipment nicht Halt gemacht. Drohnen, Flugzeuge, Panzer sind die offensichtlichsten Elemente, die davon profitieren können. Sie alle greifen auf elektronische Mechanismen zurück, die eine Orchestrierung und Nutzung entweder hochgradig optimieren oder gar erst ermöglichen. Hacking-Angriffe auf diese Komponenten sind von enormer Wichtigkeit, können Verbände massgeblich schwächen. Sie sind also zu einem elementaren Mittel in der Kriegsführung geworden. Ein Krieg kann heutzutage durchaus mit Cyber entschieden werden. Das darf man weder unterschätzen noch ignorieren.


Marc Ruef

next gen vulnerability intelligence

VulDB

Den Gegner verstehen

Tägliche Dokumentation neuer Schwachstellen, detaillierte Analyse der technischen Hintergründe, exklusive Details zu Exploiting und Gegenmassnahmen. Mit vuldb.com erhalten Sie ein durchschlagskräftiges Werkzeug in die Hand!

)SCIP(
official data provider

https://vuldb.com

MICHÈLE TREBO

DAS BEDEUTET CYBER-TERRORISMUS FÜR DIE SCHWEIZ

Cyber-Terrorismus gehört gemäss der *Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken* (NCS) zur Gruppe der *Cyber-Angriffe*. Dabei definiert sie einen Cyber-Angriff als beabsichtigte unerlaubte Handlung einer Person oder einer Gruppierung im *Cyber-Raum*, um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten zu beeinträchtigen.

Der Cyber-Terrorismus bezeichnet eine terroristisch motivierte Tätigkeit, um im Cyber-Raum das Funktionieren von Informations- und Kommunikationstechnologien zu stören oder zu zerstören, was auch physische Auswirkungen haben kann. Ziel ist es, einen möglichst grossen Schaden anzurichten, mit welchem Macht demonstriert und eine ganze Gesellschaft eingeschüchtert und destabilisiert werden soll. Dabei wird zwischen dem "reinen" Cyber-Terrorismus und dem Hilfs-Cyber-Terrorismus unterschieden. Der "*reine*" *Cyber-Terrorismus* bezeichnet terroristische Aktionen, die mit Computertechnologien und virtuell erfolgen, wohingegen der *Hilfs-Cyber-Terrorismus* zwar IT nutzt (durch IT unterstützte Attentate, Propaganda und Kommunikationsstrukturen für Terrorzellen), aber keine virtuellen Angriffe umfasst. Mit der stetig wachsenden Digitalisierung steigt auch in der Schweiz das Risiko von Cyber-Angriffen.

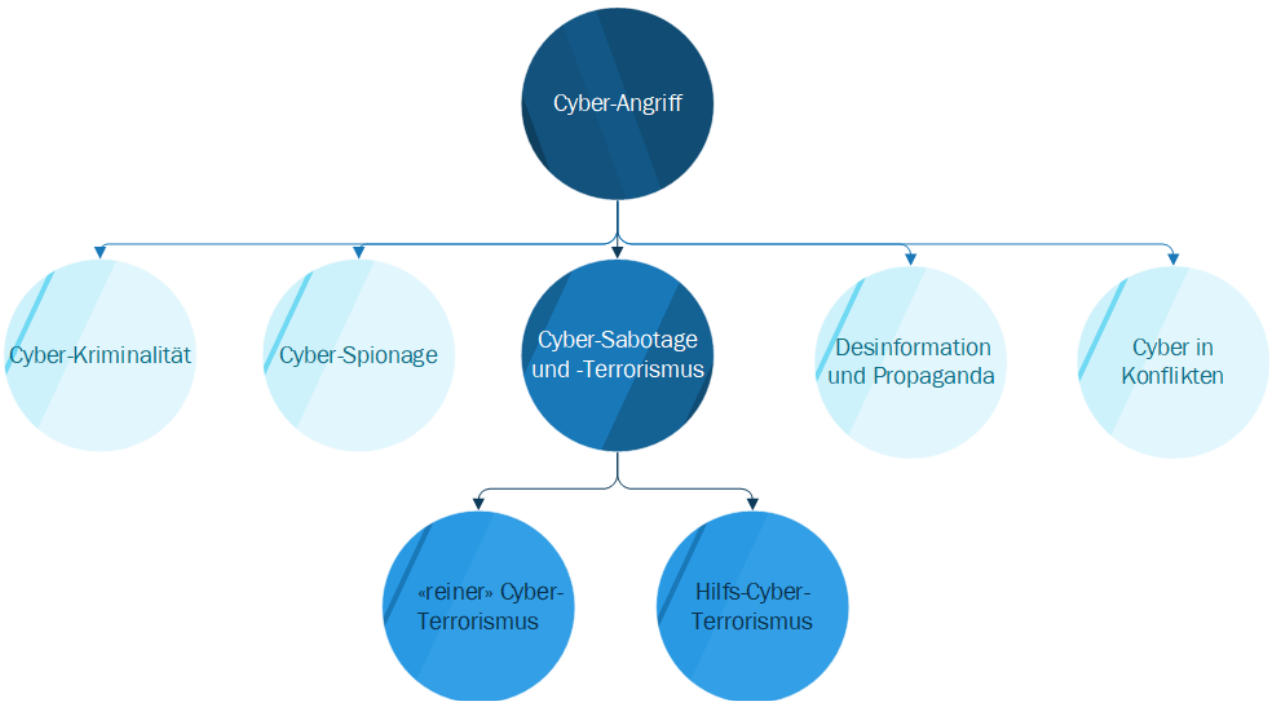
CYBER-ANGRIFFE

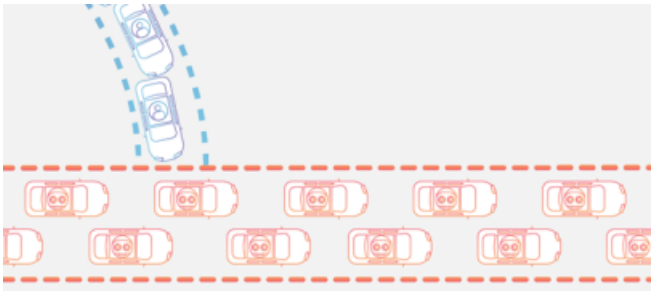
Mitte 2021 veröffentlichte *TEN.info* eine Liste der zehn weltweit grössten Cyber-Angriffe. An der Spitze die beiden Computerwürmer *NetSky* und *Sasser*, die im Jahr 2005 DDoS-Angriffe verübten. Bei einem *Denial-of-Servive-Angriff* (DDoS) wird der Zielserver, der Zieldienst oder das Zielnetzwerk mit Internet-Verkehr überlastet, sodass das Erreichen des Ziels gestört wird.

Ähnlich, wie wenn der normale Strassenverkehr aufgrund eines Staus auf der Autobahn sein Ziel nicht erreichen kann. Von den Computerwürmern NetSky und Sasser waren Computer von Banken, Reiseunternehmen und öffentlichen Einrichtungen weltweit betroffen und richteten einen Schaden von ca. 55 Milliarden Dollar an. Ein weiterer Cyber-Angriff war der Ransomware-Angriff *WannaCry* im Jahr 2017. Dabei erpressten Cyberkriminelle mithilfe von Crypto-Ransomware über vier Milliarden Dollar. *Crypto-Ransomware* verschlüsselt Daten und macht sie damit unlesbar. WannaCry nutzte eine Schwachstelle

im Betriebssystem Microsoft Windows und forderte für die Entschlüsselung der Daten Lösegeld in Form von Bitcoins. Wurde das Lösegeld in der Höhe von 300 Dollar nicht bezahlt, so wurde es auf das Doppelte erhöht. Zahlten die Betroffenen nicht binnen drei Tage, mussten sie mit der dauerhaften Löschung ihrer Daten rechnen. Forscher sind sich uneinig, ob überhaupt jemand seine Daten wieder zurückerhalten hat. Fakt ist, dass eine Zahlung an die Cyberkriminellen nicht die Freigabe der Daten garantierte. Schätzungen zufolge entstand dabei ein Schaden in der Höhe von vier Milliarden Dollar.

An der Spitze der weltweit grössten Cyber-Angriffe befindet sich zudem der *Cyber-Raub der Bangladesh Bank*. Im Jahr 2016 wurde das SWIFT-Netzwerk mittels *Malware* infiltriert und insgesamt 35 betrügerische Transaktionen ausgelöst. Fünf dieser Transaktionen gelangen. Dabei wurden von der Federal Reserve Bank of New York, bei der Bangladesch ein Konto in Dollar unterhielt, 20 Millionen Dollar nach Sri Lanka und 81 Millionen Dollar auf die Philippinen überwiesen. Die restlichen 30 Transaktionen über 850 Millionen Dollar konnten rechtzeitig als betrügerisch erkannt und gestoppt werden. Von den insgesamt illegal erworbenen 101 Millionen Dollar konnten 63 Millionen Dollar nicht mehr zurückgeholt werden. Dieser Cyber-Angriff führte nicht nur zu einem weitreichenden Verlust von Geld, sondern auch zu wirtschaftlichen Schäden und Störungen auf der ganzen Welt. Auch wenn den erwähnten Cyber-Angriffen kein terroristischer Gedanke zugrunde lag,





hatten sie allesamt grosse Auswirkung auf die Gesellschaft und richteten beträchtlichen Schaden an.

"Reiner" Cyber-Terrorismus

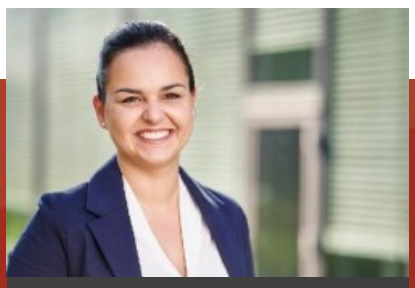
Im Jahr 2016 wurde in den Vereinigten Staaten die erste Person wegen Cyberterrorismus angeklagt. Sie wurde beschuldigt, im Jahr 2015 zusammen mit ihren Komplizen persönliche Daten von mehr als 1300 Angehörigen des US-Militärs und der Regierung gestohlen und an den Islamischen Staat weitergegeben zu haben. Die Liste dieser Daten wurde kurz darauf im Namen der *Hacking-Division des Islamischen Staates* (ISHD) unter *Kill List* veröffentlicht. Es stellte sich allerdings heraus, dass die Daten nicht aus Cyber-Angriffen sondern aus *detaillierten Open-Source-Recherchen* stammten. Im gleichen Jahr starteten terroristische Gruppierungen mit *DDoS-Angriffen*, die vor allem auf den Nahen Osten abzielten. Diese Angriffe bewirkten allerdings lediglich, dass Webseiten kurzzeitig vom Netz genommen wurden. Dem *Tunisian Fallaga Team* gelang es, die Webseite des britischen National Health Service (NHS) zu verunstalten und grausame Bilder des syrischen Bürgerkrieges anzuzeigen. Obwohl die Besorgnis über potenziellen Cyberterrorismus in den letzten Jahren aufgrund der stetig wachsenden Digitalisierung zugenommen hat, sind Cyber-Angriffe, die grosse Schäden verursacht haben, kaum auf terroristische Organisationen zurückzuführen.

Hilfs-Cyber-Terrorismus

Ende der 90er-Jahre, als das Internet noch als anonym galt, nutzten *terroristische Organisationen* Webseiten, Foren und andere Plattformen, um rasch und günstig an neue Anhänger zu gelangen. Nachdem der Islamische Staat im Jahr 2014 das Kalifat ausrief, nahm die Anzahl terroristischer Organisationen und deren Anhänger zu. Die Verbreitung von Informationen, Ratschlägen und Texten war durch *verschlüsselte Messaging-Applikationen* wie Telegram ein Kinderspiel und damit auch die Radikalisierung von Personen aus aller Welt. Es gibt Hinweise darauf, dass Terroranschläge vermehrt über *soziale Medien*, das *Darkweb* und wie bereits erwähnt Messaging-Applikationen geplant wurden. Anschläge konnten sozusagen von den Drahtziehern ferngesteuert werden.

ZUSAMMENFASSUNG

Auch wenn der Cyber-Terrorismus direkt nicht unbedingt eine grosse Gefahr für die Schweiz darstellt, muss sich die Schweiz darauf einstellen, dass aufgrund der stetig sich weiterentwickelnden Digitalisierung vermehrt Cyber-Angriffe stattfinden werden und sich überlegen, wie sie dagegen vorgehen bzw. sich davor schützen kann. Besonders bei einem Cyber-Angriff auf Behörden, Grossfirmen oder das Gesundheitswesen könnte innert kürzester Zeit die Infrastruktur der Schweiz still gelegt werden und massive Schäden zur Folge haben.



Michèle Trebo

DATEN SIND STETS IM FLUSS

Bildquelle: https://pixabay.com/images/id-7047522/

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch