MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE OKTOBER 2021
RANSOMWARE AND CIS CONTROLS

SO REAGIEREN SIE AUF RANSOMWARE

Ransomware-Attacken sind eine drohende Gefahr, die sich als lukratives Geschäftsmodell etablieren konnte. Unser Incident Response Handbuch hilft Ihnen, mit dieser Bedrohung umzugehen.

NEUERUNGEN DER CIS CONTROLS V8

Die jüngsten CIS-Kontrollen wurden um aktuelle Themen und Arbeitsweisen ergänzt und setzen die aus früheren Versionen bekannten Grundsätze konsequent fort. Unkompliziert erhalten Sie einen Überblick der neuen V8.

Oktober 2021: Nie ohne Logs

Auf das Einsetzen von Log-Dateien wird gerne verzichtet. Schliesslich erfordern die zusätzlichen Schreibprozesse wiederum Taktzyklen, die den Berechnungen gestohlen werden würden. Zudem ist (Festplatten-)Speicher begrenzt und man will ja schliesslich nicht unnötig irgendwelche Daten bunkern. Den Computer und seine Ressourcen will man schonen.

Doch kommt es zu Problemen, dann steht man nun plötzlich auf verlorenem Posten. Das Fehlen eines umfassenden und zuverlässigen Loggings kann dazu führen, dass sich Fehlerquellen nicht zurückverfolgen und identifizieren lassen. Man ist quasi blind - Die Auswirkungen des Fehlers versperren einem die Sicht auf die Wurzel dessen.

Wirklich problematisch wird es, wenn ein elektronischer Einbruch gegeben ist und eine forensische Analyse ansteht. Der Forensiker ist im schlimmsten Fall weder in der Lage eine Spurensicherung zu machen (es sind keine Spuren da) und damit ist auch keine Analyse dieser umsetzbar. Eine sehr unangenehme Situation, die die ansonsten schon schwer handelbaren Zustände noch schwerer macht.

Nur wenige Leute in der IT-Industrie haben begriffen, wie wichtig ein durchdachtes Log-Management wirklich ist. Schon nur einfache Lösungen können in hektischen Situationen zum goldenen Vorteil werden. Wirklich elegant und effizient kann man einer Lage aber erst Herr werden, wenn da denn zentralisierte und normalisierte Systeme zum Einsatz kommen, dank deren Hilfe man innert kürzester Zeit Überblick der Situation erhalten und die Quellen der Probleme eruieren kann.

Marc Ruef
Head of Research

NEWS

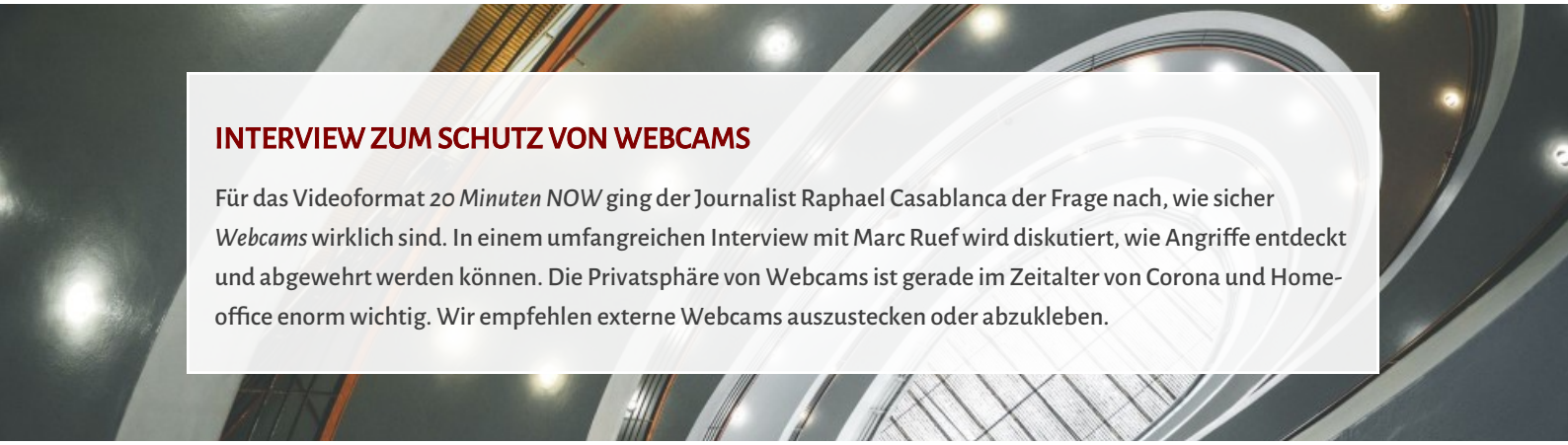
WAS IST BEI UNS PASSIERT?

TOMASO VASELLA WIRD NEUER CEO DER SCIP AG

Tomaso Vasella wird ab dem 1. Oktober 2021 neuer *CEO der scip AG*. Firmengründer Simon Zumstein fokussiert sich auf die Strategie und wird Verwaltungsratspräsident. Die scip AG, seit 2002 als *Pionier im Bereich IT-Security* tätig, hat sich mit ihren drei Geschäftsbereichen *Red* (Offensive Security), *Blue* (Defensive Security) und *Titanium* (Research) erfolgreich als qualitativ hochstehendes und führendes Unternehmen etabliert.

EXPERTENKOMMENTARE ZU FACEBOOK-DATENSAMMLUNG

Im Rahmen unseres *Darknet-Monitorings* haben wir Anfang September aufgedeckt, dass die grösste bisher bekannte *Facebook-Datensammlung* gehandelt wird. Die 1.5 Milliarden Datensätze haben mittlerweile das Interesse der Medien entdeckt, die zum Fall berichten. Darunter *Russia Today* und *News 24*.Die Daten wurden im Rahmen der öffentlich verfügbaren, aber dennoch suboptimal abgesicherten API, abgegriffen.



INTERVIEW ZUM SCHUTZ VON WEBCAMS

Für das Videoformat *20 Minuten NOW* ging der Journalist Raphael Casablanca der Frage nach, wie sicher *Webcams* wirklich sind. In einem umfangreichen Interview mit Marc Ruef wird diskutiert, wie Angriffe entdeckt und abgewehrt werden können. Die Privatsphäre von Webcams ist gerade im Zeitalter von Corona und Homeoffice enorm wichtig. Wir empfehlen externe Webcams auszustecken oder abzukleben.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

VERÖFFENTLICHUNG DES NEUEN JAHRBUCHS

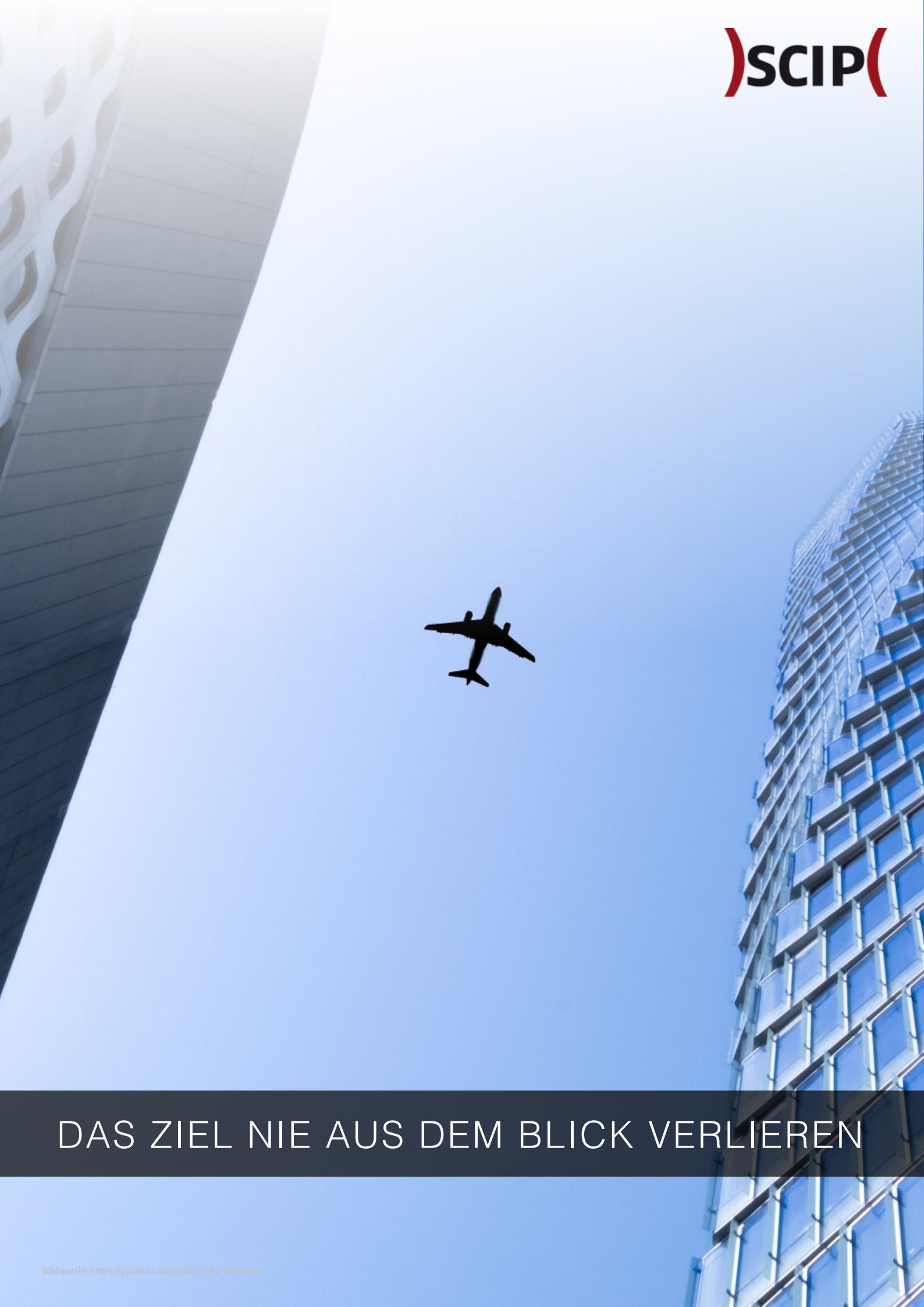
Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 11ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

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]



DAS ZIEL NIE AUS DEM BLICK VERLIEREN

Bildquelle: https://pixabay.com/images/id-6674689/

MARC RUEF

SO REAGIEREN SIE AUF RANSOMWARE

Ransomware gibt es seit den 1980er Jahren. Doch erst durch die Verbreitung des Internets konnte dieses kriminelle Geschäftsmodell an Popularität gewinnen. Mit der medialen Aufmerksamkeit, die dem Thema durch *WannaCry* im Mai 2017 entgegengebracht wurde, wurde diese Angriffsmöglichkeit zu einem festen Bestandteil moderner Cybersecurity.

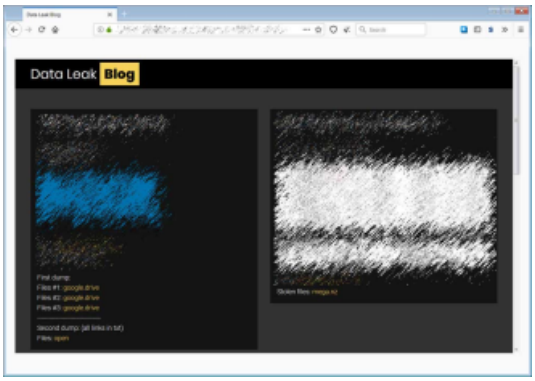
Eine Vielzahl an Firmen sehen sich dieser Bedrohung und den mit ihr einhergehenden Schäden konfrontiert. Dabei wird durch die Betroffenen in der Hitze des Gefechts oftmals *falsch* reagiert. Dieser Beitrag diskutiert das richtige strategische und taktische Vorgehen bei einem *Ransomware-Befall*. Viele Aspekte hiervon können ebenfalls auf Erpressung mittels klassischen *DDoS-Attacken* (Distributed Denial of Service) angewendet werden.

STRATEGIE VON RANSOMWARE

Bei *Ransomware* handelt es sich um eine spezielle Klasse von *Malware*. Ransomware ist darum bemüht ein System zu *infizieren*, um durch weitere Massnahmen *Geld zu erpressen*. Traditionell geschieht dies durch die *Verschlüsselung der Daten*. Die Datenbesitzer können auf diese erst wieder zugreifen, wenn ein entsprechendes Lösegeld bezahlt wird. Nach erfolgreicher Transaktion, die oftmals durch Bitcoin oder alternative Kryptowährungen umgesetzt werden will, wird dem Opfer der Schlüssel zur Entschlüsselung ausgehändigt. Falls eine Zahlung ausbleibt, bleiben die Daten "für immer Verschlüsselt" oder werden irgendwann gar aktiv gelöscht.

Bei einer *Double-Extortion* werden die Daten, bevor sie verschlüsselt werden, entwendet. Damit kann durch die Täterschaft ein zusätzlicher Hebel etabliert werden: Findet die Lösegeldzahlung nicht statt – da zum Beispiel dank eines zuvor angefertigten Backups auf die Daten zugegriffen werden kann -, wird eine Veröffentlichung dieser angedroht. Dies ist vor allem dann problematisch, wenn es sich um sensitive (z.B. Finanzdaten, Intellectual Property) oder persönliche Daten (z.B. Kundeninformationen) handelt.

Auf der Basis eines solchen Datendiebstahls kann ebenfalls eine *Triple-Extortion* angestrebt werden. Falls persönliche Daten enthalten sind, werden zusätzlich die betroffenen Personen erpresst. Dabei kann es sich sowohl im Mitarbeiter als auch Kunden handeln. Problematische Beziehungen (z.B. zu Ban-



ken) oder kompromittierende Informationen (z.B. Patientendaten) lassen sich nutzen, um die Daten zu Geld zu machen. Die angedrohte Veröffentlichung der Daten geschieht auf den *Data Leak Sites* der Ransomware-Gangs, in Foren für Datenhandel, auf Filesharing-Plattformen oder durch öffentliche Torrents.

PHASE 1: ENTDECKUNG DER RANSOMWARE

Als erstes gilt es einen Ransomware-Befall zu *entdecken*. Dies geschieht im Idealfall durch bestehende und funktionierende technische Hilfsmittel. Dazu gehören typischerweise:

- Antiviren-Lösungen (AV)
- Firewalls (FW)
- Intrusion Detection-Systeme (IDS)
- Intrusion Prevention-Systeme (IPS)
- Data Loss Prevention-Systeme (DLP)
- Logging und Monitoring (z.B. Dateizugriffe, Systemauslastung, Bandbreitennutzung)

Ransomware wird grösstenteils mit Standard-Produkten umgesetzt, die durch entsprechende Sicherheits-Lösungen wie AV, FW, und IDS erkennt werden können. Falls zudem eine Exfiltration unüblich grosser Datenmengen stattfindet, können DLP, Logging und Monitoring anschlagen. Falls solche Mechanismen nicht vorhanden, fehlerhaft implementiert oder falsch konfiguriert sind, kann eine Entdeckung ausbleiben, wodurch eine Kompromittierung erst möglich wird. Einzelne oder gar alle diese Mechanismen gelten jedoch in der heutigen Zeit als Good Practice.

Warnmeldung von WannaCry

Nachdem eine Ransomware die Infektion, Rechteausweitung, Kompromittierung und Exfiltration der Daten erfolgreich umgesetzt hat, macht sie sich in der Regel bemerkbar. Dies geschieht typischerweise durch eine Meldung auf dem Bildschirm der betroffenen Systeme. Manche Ransomware-Gangs pflegen aber auch Kontakt per Email zu den Opfern aufzunehmen.

PHASE 2: UMGANG MIT DEN ERPRESSERN

In jedem Fall gilt es, mindestens zu Beginn, den Kontakt und Austausch mit den Erpressern zu vermeiden. Eine Reaktion jeglicher Art sollte ausbleiben. Dazu gehört ebenfalls ein freundliches: "Vielen Dank, wir klären ab und melden uns wieder."

Es geht darum, dass die Täterschaft vorerst nicht weiss, ob die Infektion wirklich erfolgreich war, diese einen konkreten Schaden verursachen konnte, ihr Anliegen der Erpressung und diese als konkrete Bedrohung wirklich wahrgenommen wurde. Dadurch kann zeit gewonnen sowie die Täter zu weiteren Abklärungen und einer erneuten Kontaktaufnahme gezwungen werden.

Die gewonnene Zeit kann für das Ausarbeiten und Umsetzen weiterer Massnahmen genutzt werden. Zudem macht eine zähe Kommunikation das Opfer zu einem weniger lohnenden Angriffsziel. Die Täter müssen ein Mehr an Aufwand investieren, um an ihr Ziel zu kommen. Im Sinne der Wirtschaftlichkeit wünschen sie sich jedoch Verhandlungspartner, die zügig und unkompliziert kooperieren.

Dabei ist aber wichtig sicher zu sein, dass man die Möglichkeiten der Ransomware und die bisher durchgeführten Kompromittierungsschritte zweifelsfrei nachvollziehen kann. Durch das Auswerten der Logs für Dateizugriffe und Netzwerkübertragungen muss nachgewiesen werden können, dass keine Exfiltration von Daten durchgeführt wurde. Dadurch kann das Risiko einer Double- oder Triple-Extortion verhindert werden. Falls sich eine solche abzeichnet, wird je nachdem dennoch ein Austausch mit den Erpressern erforderlich.

Von einer *Zahlung* sollte stets abgesehen werden. Wenn eine solche ausgeführt wird, kann im Idealfall die Erpressung beendet sein. Es ist aber nicht ausgeschlossen, dass eine solche nur *aufgeschoben* und stattdessen in absehbarer Zeit eine *neue Forderung* gestellt wird. Im Gegensatz kann bei einer Geiselnahme durch einen Austausch die konkrete Gefahr für Leib und Leben der Geisel aufgehoben werden. Bei Verschlüsselung und Datendiebstahl ist man sich – mindestens vorerst – nicht sicher, ob bei einer Zahlung die Gefahr wirklich nachhaltig gebannt wurde: Ist das System nicht doch noch infiziert, werden die Kopien der gestohlenen Daten wirklich vernichtet, wird von einem Gang zu den Medien abgesehen? In

den meisten Fällen ist die Gefahr nicht gebannt und kann auch nicht mit absoluter Gewissheit als solche gewährleistet werden. Durch eine Zahlung zeigt man sich in erster Linie willig, auf Forderungen einzugehen.

Zahlungen sind nur dann anzuraten, wenn durch diese *zwingend benötigte Zeit* gewonnen werden kann. Also wenn sich das Zeitfenster für eine Vernichtung oder Veröffentlichung der Daten schliesst, man aber nachhaltige Massnahmen noch nicht umfangreich etablieren konnte. Eine Lösegeldzahlung muss immer in einem weitreichenden Plan eingebettet sein. In den USA wird gegenwärtig diskutiert, ob Ransomware-Zahlungen *unter Strafe gestellt* werden sollen.

Die meisten Ransomware-Gangs arbeiten zuverlässig, wenn es um Zahlungen und damit erkaufte Datenfreigaben handelt. Wird nämlich bekannt, dass eine getätigte Zahlung die Drohungen nicht abwenden kann, pulverisiert sich unmittelbar ihr Geschäftsmodell. Denn niemand wird von nun an mehr gewillt sein, solche Zahlungen ohne Gegenwert vorzunehmen.

Die defensive Cybersecurity-Community ist stets darum bemüht, durch ein Reverse Engineering der Ransomware ihre Funktionsweise verstehen und eigene Decryption-Keys generieren zu können. Es ist nicht unüblich, dass nach Wochen oder spätestens Monaten für bekannte Ransomware-Familien entsprechende Decryption-Keys eigenmächtig erstellt werden.

PHASE 3: ALARMIERUNG DER BEHÖRDEN

Einzelne Ransomware-Gangs drohen damit, konkrete Schäden anzurichten, falls die Behörden oder Cybersecurity-Firmen hinzugezogen werden. Entsprechend ist ein diskretes und zielgerichtetes Vorgehen angeraten.

Spätestens wenn sich eine Infektion als Erpressungsversuch offenbart, müssen die entsprechenden Stellen informiert werden. Die Cybersecurity-Abteilung des Unternehmens sollte sich mit dem *Nationalen Zentrum für Cybersicherheit* (NCSC) in der Schweiz oder dem *Bundesamt für Sicherheit in der Informationstechnik* (BSI) in Deutschland in Verbindung setzen.

Diese sind in der Regel um laufende Ransomware-Kampagnen informiert, können die Situation und Täterschaft einschätzen. Durch sie kann ein *Coaching* erfolgen, wie auf technischer und verhandlungstechnischer Ebene vorgegangen werden soll. Externe Cybersecurity-Firmen sollten beigezogen werden, um die empfohlene Vorgehensweise professionel umsetzen zu können.

Zudem sollte zu einem späteren Zeitpunkt (erst wenn Phase 4 erfolgreich angelaufen ist) eine *Anzeige bei der Polizei* erstattet werden. Dies kann regulär bei einem Polizeiposten gemacht werden. Lassen Sie sich nicht durch die Beamten entmutigen, dass eine solche Anzeige sinnlos sei und keine Resultate zu Tage fördern wird. Das Befolgen dieser Rechtsbelehrung hilft in erster Linie den Tätern. Das Aufgeben einer Anzeige gegen Unbekannt ist an keine Voraussetzungen geknüpft. Sie kann ebenso erforderlich werden, um beispielsweise von der Deckung durch eine *Cyberversicherung* Gebrauch machen zu können.

PHASE 4: UMSETZEN TECHNISCHER MASSNAHMEN

Eine Ransomware-Erpressung kann nur funktionieren, wenn sich diese auf technischer Ebene erfolgreich manifestieren konnte. Entsprechend wird es unmittelbar wichtig, dass ihr auf technischer Ebene entgegnet werden kann.

Als erstes muss eine *Identifikation* der Malware-Familie, ihrer *Funktionsweise und Möglichkeiten* umgesetzt werden. Viele Ransomware-Produkte weisen sich mit eindeutigen Namen aus. Durch eine Internet-Recherche lässt sich unkompliziert herausfinden, was diese genau macht. Dabei ist es nicht unüblich, dass eine Malware durch die verschiedenen Antiviren-Hersteller unterschiedliche Namen mitgegeben wird.

Durch die Identifikation lässt sich ableiten, welcher *Schaden* besteht oder droht: Was und wie wird etwas tangiert? Die betroffenen Systeme und Daten lassen sich meist schnell ausfindig machen. Nun gilt es zu entscheiden, welcher *Wert diesen Daten* beigemessen werden soll. Falls sie nicht erforderlich oder leicht ersetzbar sind, wird der direkte Umgang mit den

Erpressern nicht mehr erforderlich sein. Es ist anzuraten, dass ein *durchdachtes Backup-Konzept* zum Tragen kommt, bei dem im Idealfall ein Offline-Backup mitberücksichtigt wird.

In jedem Fall muss herausgefunden werden, wie die *Infektion und Kompromittierung* stattfinden konnte. Welche Systeme sind betroffen, wie wurde die Ransomware eingeschleust. Oftmals sind es fehlende Patches, Fehlkonfigurationen oder Fehlmanipulationen durch Benutzer (z.B. Öffnen eines Mail-Attachments oder Einstecken eines infizierten USB-Sticks). Die identifizierten Lücken müssen geschlossen werden, um eine erneute und zukünftige Kompromittierung ausschliessen zu können. Falls infizierte Systeme über einen Wurm die umliegenden Systeme im gleichen Netzwerk infizieren, müssen die betroffenen Systeme isoliert (vom Netz getrennt) werden.

Die beeinträchtigen Komponenten, namentlich die veränderten bzw. verschlüsselten Daten, sollten *gerettet* werden. Am einfachsten kann dies durch das Wiederherstellen eines zuvor erstellen *Backups* geschehen. Dabei gilt es darauf zu achten, dass ein einwandfreies Backup eingespielt wurde, das nicht schon kompromittiert werden konnte. Dadurch kann der normale Betriebszustand wieder hergestellt werden.

PHASE 5: BEKANNTMACHUNG DES ZWISCHENFALLS

In einem letzten Schritt muss sich um die *Kommunikation des Vorfalls* gekümmert werden. Gesetzliche Bestimmungen können es erforderlich machen, dass Behörden und/oder Kunden innert einer vordefinierten Zeitspanne über den Zwischenfall informiert werden müssen. Namentlich steuert dies das *Bundesgesetz über den Datenschutz* (DSG) in der Schweiz sowie die *Datenschutz-Grundverordnung der Europäischen Union* (DSGVO). Falls eine solche Benachrichtigung ausbleibt, können rechtliche Aufwände und finanzielle Schäden drohen.

Mit einer auf Datenschutz spezialisierten Anwaltskanzlei muss eine Bewertung der tangierten Daten erfolgen, um die rechtlichen Reaktionen bestimmen und planen zu können. Die Kommunikation mit den betroffenen Kunden muss *zeitnah und ehrlich* erfolgen. Diese Leute sind auf Grund des Verschuldens des Anbieters zu Schaden gekommen oder sehen

sich zukünftigen Gefahren des Datenmissbrauchs ausgesetzt. Sie durch marketinggetriebene Floskeln zu verärgern wird zu Vertrauensverlust und Unmut führen. Behaupten Sie nie, dass persönliche Daten nicht wirklich sensitiv seien. Ihre Kunden werden das definitiv anders sehen.

Art. 33 Abs. 1 DSGVO sieht eine Dokumentation und Meldung an die zuständige Aufsichtsbehörde vor. Bei einem Risiko für "Rechte und Freiheit" hat dies innerhalb von 72 Stunden zu erfolgen. Art. 34 Abs. 1 DSGVO regelt, dass Kunden ebenfalls informiert werden müssen. Tangiert es ihre "Rechte und Freiheit", dann muss dies unverzüglich geschehen. Und laut Art. 34 Abs. 2c DSGVO hat gar eine öffentliche Bekanntmachung zu erfolgen. Falls die Vorgaben der DSGVO nicht eingehalten werden, kommen Art. 58 Abs. 2 sowie Art. 83 DSGVO zum Tragen. Säumige werden dann mit einer Strafe bis zu 20 Millionen Euro oder 4% des Umsatzes des Vorjahres, es wird der höhere Richtwert als Ausgangslage genommen, belegt.

Von einer aktiven Bekanntmachung des Zwischenfalls in den Medien ist bei fehlendem öffentlichen Interesse nach Möglichkeiten abzusehen. Dabei geht man jedoch das Risiko ein, dass wenn der Fall anderweitig an die Öffentlichkeit getragen wird, die Krisenkommunikation in Frage gestellt wird. Das gleiche Prinzip der ehrlichen Kommunikation muss also auch im Umgang mit den Medien befolgt werden. Statements müssen professionell sein. Inhaltslose Floskeln, technische Fehleinschätzungen oder gar überhebliche Ignoranz werden zu einem nachhaltigen Reputationsschaden führen.

Es kann ein *PR-Beratungsunternehmen* beigezogen werden, das die Kommunikation vorantreibt. Dieses muss aber auf Krisenkommunikationen im IT-Bereich spezialisiert sein. Andernfalls können die zuvor skizzierten Anforderungen an die Professionalität bei weitem nicht erreicht werden. Schlechte Beispiele gab es in der Vergangenheit zu Hauf.

Es gilt immer zu bedenken, dass das betroffene Unternehmen *mitschuldig am Zwischenfall* ist. Es waren fehlende oder fehlerhafte Sicherheitsmassnahmen, die einen erfolgreichen Angriff erst ermöglicht haben. Art. 7 Abs. 1 DSG zeigt die Mitschuld klar auf:

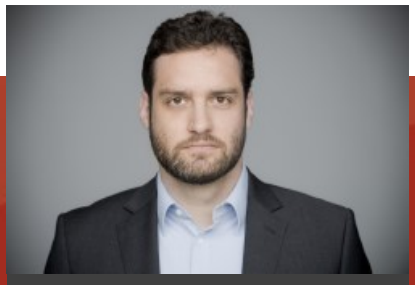
> *Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.*

Ob strategische, technische oder personelle Fehlbarkeiten zum Problem geführt haben, ist im Rahmen der Kommunikation nicht relevant. Diese aber abzustreiten und stattdessen der Täterschaft eine "nicht abwehrbare Professionalität" zu attestieren, kann und wird sowohl von Kunden als auch den Medien als Dreistigkeit wahrgenommen werden.

Stattdessen sollte man sich auf die Fakten fokussieren. Dabei sollte nur das kommuniziert werden, was für die Öffentlichkeit auch von Nutzen ist. Die Preisgabe von Informationen darf keinen Schaden für das Unternehmen mit sich führen. Falls zum Beispiel eine Lösegeldzahlung geleistet wurde, darf diese *unter keinen Umständen* bekannt werden. Falls sie an die Öffentlichkeit dringt, wird man zu einem lohnenden Ziel für Nachahmungstäter.

FAZIT

Ransomware-Attacken sind eine drohende Gefahr, die sich als lukratives Geschäftsmodell etablieren konnte. Komplexitäten und Abhängigkeiten führen zu einer Zunahme entsprechende Kompromittierungen. Dabei ist es wichtig, anhand des geschilderten 5-Phasen-Plans vorzugehen, um zu jeden Zeitpunkt eine weitsichtige und damit professionelle Vorgehensweise verfolgen zu können. Dies beginnt bei der technischen Analyse der Ransomware und endet bei der Kommunikation mit Kunden und Medien. Strategische und taktische Fehler können sich rächen und zu einem Mehr an Schaden führen.



Marc Ruef

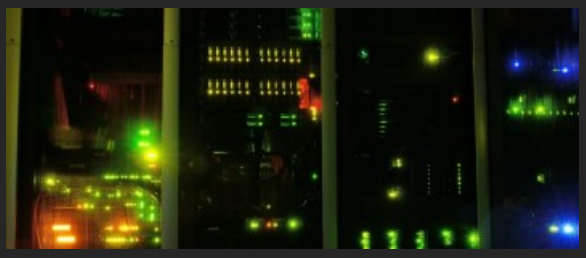
UNSERE SPEZIALISTEN SETZEN SICH TÄGLICH MIT DEM THEMA CYBERSECURITY AUSEINANDER. DIESER ERFAHRUNGSSCHATZ LÄSST KEINEN ZWEIFEL DARAN, DASS

WIR ÜBERZEUGEN

UND INSPIRIEREN KÖNNEN. BUCHEN SIE UNS FÜR IHREN EVENT, DAMIT WIR AUCH IHR PUBLIKUM MITREISSEN UND FÜR DAS THEMA BEGEISTERN KÖNNEN.

CYBERCRIME & DARKNET

Das Darknet gilt als verborgener Bereich des Internets, der durch Cyberkriminelle genutzt wird und schwierig zugänglich ist. Wir zeigen anhand konkreter Fälle, wie man sich im Darknet bewegt.

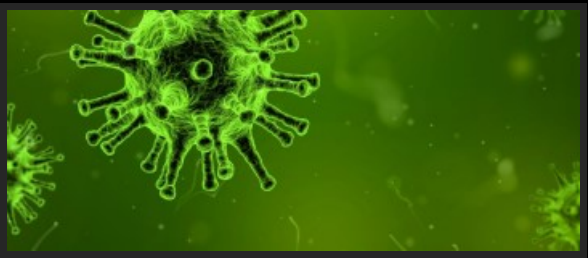


INTERNET OF THINGS

Das Thema IoT schleicht sich in unseren Alltag und beginnt uns zu beherrschen. Welche verheerenden Folgen Angriffe auf die digitale Infrastruktur haben, zeigen unsere aktuellen Forschungsresultate.

ARTIFICIAL INTELLIGENCE

Künstliche Intelligenz beginnt immer mehr Einfluss auf unser tägliches Leben zu nehmen. Die dadurch gewonnenen Chancen bringen aber auch Risiken mit, wie wir an konkreter Forschung illustrieren können.



MALWARE & RANSOMWARE

Unser Red Team führt offensive Penetration Tests durch, bei denen individuelle Malware für den Kunden entwickelt wird. Unser Wissen zeigt konkret, wie böswillige Viren-Entwickler denken und handeln.

Weitere Informationen auf unserer Webseite

www.scip.ch

TOMASO VASELLA

WAS IST NEU IN DEN CIS CONTROLS V8

Cybersecurity-Vorfälle gehören inzwischen immer mehr zum Alltag und müssen leider schlicht als Teil der Normalität betrachtet werden. In den letzten Jahren hat eine starke Professionalisierung der Angreifer stattgefunden und die Zahl der Angriffsziele ist durch fortschreitende Digitalisierung stark gestiegen – eine Entwicklung, die auch in den kommenden Jahren anhalten dürfte. Gleichzeitig sind sich immer mehr und auch kleinere Organisationen der Bedrohungen und der Notwendigkeit robuster Sicherheitsmassnahmen bewusst.

Diese Entwicklungen führen auch zu einer zunehmenden *Vielfalt* von *Sicherheitsstandards*, *Regulativen*, *Richtlinien* und *Hilfsmitteln*, die Organisationen aller Grössen dabei helfen sollen, Risiken richtig einzuschätzen und *wirksame Massnahmen* für einen angemessenen Schutz zu ergreifen. Einerseits ist dies begrüssenswert, andererseits existieren inzwischen fast schon zu viele Sicherheitsstandards, so dass es gerade kleineren Organisationen schwerfallen kann, die essenziellen oder minimal nötigen Vorkehrungen herauszuschälen (zur Illustration können die referenzierten Standards im *Secure Controls Framework* dienen).

CIS-KONTROLLEN

Es ist eines der *Hauptziele der CIS-Kontrollen*, genau hier anzusetzen und für alle *Organisationsgrössen* und verschiedene *Sicherheitsbedürfnisse* eine *Hilfestellung* zur Verfügung zu stellen. Die CIS-Kontrollen sind eine *Sammlung* konkreter, priorisierter *Sicherheitsmassnahmen* (sogenannte Safeguards), die der Abwehr der häufigsten Cyberangriffe auf Systeme und Netzwerke dienen. Vor allem für Organisationen, die noch nicht über ein Sicherheitsprogramm verfügen, bieten sie eine wertvolle Orientierungs- und Starthilfe. Die CIS-Kontrollen referenzieren verschiedene anerkannte Frameworks wie das NIST CSF, ISO 27000, PCI DSS und weitere und bestehen aus konkreten, pragmatisch umsetzbaren Massnahmen. Die CIS-Kontrollen gibt es seit vielen Jahren und sie werden laufen weiterentwickelt und neuen Entwicklungen und Erkenntnissen angepasst.

Die CIS-Kontrollen in der *aktuellen Version 8* (früher: *CIS Critical Security Controls* oder *CIS Top 20*) wurden im Mai 2021 veröffentlicht. Sie wurden angepasst, um besser mit modernen Systemen und aktueller Software Schritt zu halten. Die fortschreitende Umstellung auf Cloud Computing, zunehmende Mobili-

tät, Telearbeit und Home-Office und auch veränderte Angriffstaktiken waren der Anlass für die Aktualisierung. Die nachfolgende Abbildung zeigt eine Übersicht über alle 18 CIS-Kontrollen.

Implementation Groups

Seit Version 7.1 definieren die CIS-Kontrollen *drei* aufeinander *aufbauende*, sogenannte *Implementation Groups* (IG). Diese Gruppen dienen vor allem der *Priorisierung* der *Sicherheitsmassnahmen*, richten sich aber auch an verschiedene Sicherheitsbedürfnisse. So fasst die IG1 diejenigen Massnahmen zusammen, die zu Erreichung eines grundlegenden Sicherheitsniveaus umgesetzt werden sollten und auch mit eingeschränkten Ressourcen und wenig Expertise erreicht werden können.

Welche weiteren Implementation Groups umgesetzt werden sollen, muss eine Organisation für sich selbst entscheiden. Diese Entscheidung sollte die folgenden Gesichtspunkte berücksichtigen:

- Risikoprofil der Organisation bzw. ihrer Geschäftstätigkeit
- Kritikalität der verarbeiteten Daten und der erbrachten Dienstleistungen
- Grösse der Organisation und verfügbare Ressourcen und Expertise

Implementation Group 1

Die *IG1* umfasst *56 Massnahmen* zur Erreichung eines *Minimalniveaus* an Informationssicherheit. Diese Massnahmen beinhalten grundsätzliche Themen und Vorkehrungen wie Inventar, sichere Konfigurationen, Zugriffskontrollen, Backup usw. Sie stellen das absolute Minimum an Sicherheitsmassnahmen dar, die jede Organisation implementieren sollte und werden dementsprechend auch als *Basic Cyber Hygiene* bezeichnet.

Implementation Group 2

Die *IG2* umfasst *74 weitere Massnahmen* und baut auf der IG1 auf. Ziel dieser Implementation Group ist die Unterstützung von etwas grösseren Organisationen, die möglicherweise aus mehreren Abteilungen mit unterschiedlichen Risikoprofilen bestehen und etwas grössere Komplexität aufweisen. Einige der Massnahmen setzen Lösungen und Werkzeuge voraus, die eher in grossen Umgebungen eingesetzt werden und Spezialisten für die Konfiguration und den Betrieb erfordern können. Beispiele sind automatisierte Lösungen für die Inventarisierung von Hard- und Software, Lösungen für das Schwachstellenmanagement oder zentralisiertes Logging und Monitoring.

Implementation Group 3

Die *IG3* umfasst *23 zusätzliche Massnahmen* und baut auf der IG2 auf. Sie sind darauf ausgerichtet, auch grössere Organisationen mit mehr Ressourcen und Sicherheitsexpertise zu einem besseren Schutz auch gegen höher entwickelte Angriffe zu verhelfen. Themen dieser Gruppe sind unter anderem verbesserte Detektionsmöglichkeiten für sicherheitsrelevante Ereignisse und umfassenderes Security Testing.

NEUERUNGEN IN DER VERSION 8

Die offensichtlichste Änderung gegenüber der Vorgängerversion ist die Reduktion auf insgesamt 18 Kontrollen mit 153 Massnahmen (Version 7.1: 20 Kontrollen und 171 Massnahmen). Dies ist einerseits einer stärkeren Fokussierung auf das heute wesentliche geschuldet, andererseits sind Themen teilweise zusammengefasst worden.

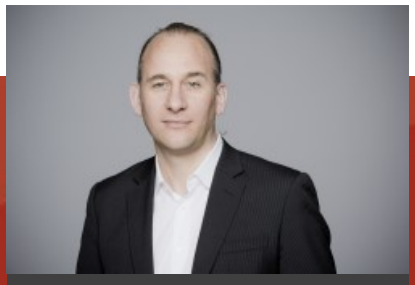
Änderungen seit der letzten Version

Neu ist das *Service Provider Management* (Kontrolle 15) hinzugekommen, was der immer noch zunehmenden Bedeutung des Cloud Computing und dem hohen Stellenwert der Sicherheit von Versorgungsketten Rechnung trägt. Auffallend, aber einleuchtend, ist auch die Verschiebung der Kontrolle “Data Protection” nach vorne auf Stelle 3 und die Erhöhung der Prioritäten der Themen “Account Management” und “Access Control Management”. Die Änderungen auf der Ebene der Kontrollen sind somit recht übersichtlich ausgefallen. Hingegen wurden auf der Ebene der

Massnahmen über 200 Änderungen vorgenommen. Organisationen, die bereits die CIS-Kontrollen einsetzen, sollten sich deshalb im Detail mit den Neuerungen auseinandersetzen. Eine umfassende Zusammenstellung aller Änderungen seit der letzten Version stellt CIS auf ihrer Website zur Verfügung.

ZUSAMMENFASSUNG

Die jüngsten CIS-Kontrollen wurden um aktuelle Themen und Arbeitsweisen ergänzt und setzen die aus früheren Versionen bekannten Grundsätze konsequent fort. Es wurde noch mehr auf die Konzentration auf das Wesentliche und auf den Einbezug von Organisationen aller Arten und Grössen geachtet. Das Konzept der Implementation Groups betont den Begriff der "Cyber Hygiene" in der Version 8 noch stärker und definiert einen Minimalstandard für Informationssicherheit, der auch für kleine Organisationen mit eingeschränktem Budget und Ressourcen erreichbar ist. Angesichts der wahrscheinlichen Entwicklungen darf man annehmen, dass heute als fortgeschritten bezeichnete Massahmen künftig nur noch zur Erreichung eines Minimalniveaus an Informationssicherheit ausreichen werden.



Tomaso Vasella

JEDER BRAUCHT MANCHMAL EINEN KLEINEN WEGWEISER

Bildquelle: https://pixabay.com/images/id-6583224/

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