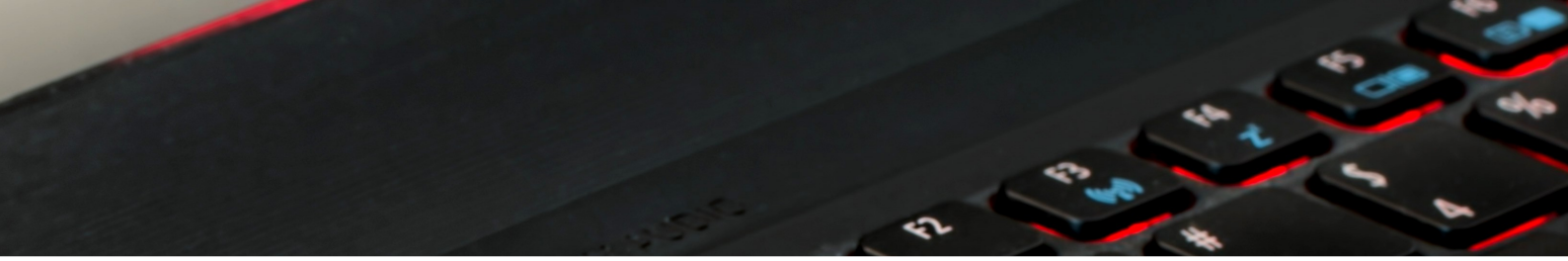


MONTHLY SECURITY SUMMARY

Ausgabe Juni 2017

Bildquelle: https://pixabay.com/photo-2301933/

FOKUS

CYBERCRIME UND ONLINE-FRAUD

Juni 2017: Sommerzeit, Betrugszeit

Sie steht uns wieder bevor, die *Ferienzeit*. Wer sich nicht gerade selber in den Bergen oder am Strand vom Arbeitsalltag erholt, der bekommt oftmals schneller als gewohnt Antwort auf E-Mails – in Form von Out-of-Office Benachrichtigungen.

Für den geneigten *Social Engineer* gibt es kaum etwas praktischeres, als relativ genaue Informationen zur sommerlichen Abwesenheit von Teamkollegen, Vorgesetzten oder anderen Bezugspersonen. Ohne saubere Übergabe, die oftmals im Stress der letzten Arbeitstage untergeht, fällt es leicht, eine Zielperson davon zu überzeugen, dass man doch diese Daten noch vom Kollegen erhalten haben müsste, aber der ja doch jetzt in den Ferien weile und sie doch so lieb sein soll, das noch nachzuholen.

Es lohnt sich also, gerade in den Sommermonaten Vorsicht walten zu lassen. Und auch ganz allgemein, möchten wir Ihre Sinne mit der vorliegenden Ausgabe einmal mehr für Betrug und kriminelle Machenschaften schärfen und wünschen Ihnen mit dem Schwerpunktthema *Cybercrime und Online-Fraud* viel Vergnügen.

Stefan Friedli
Head of Auditing

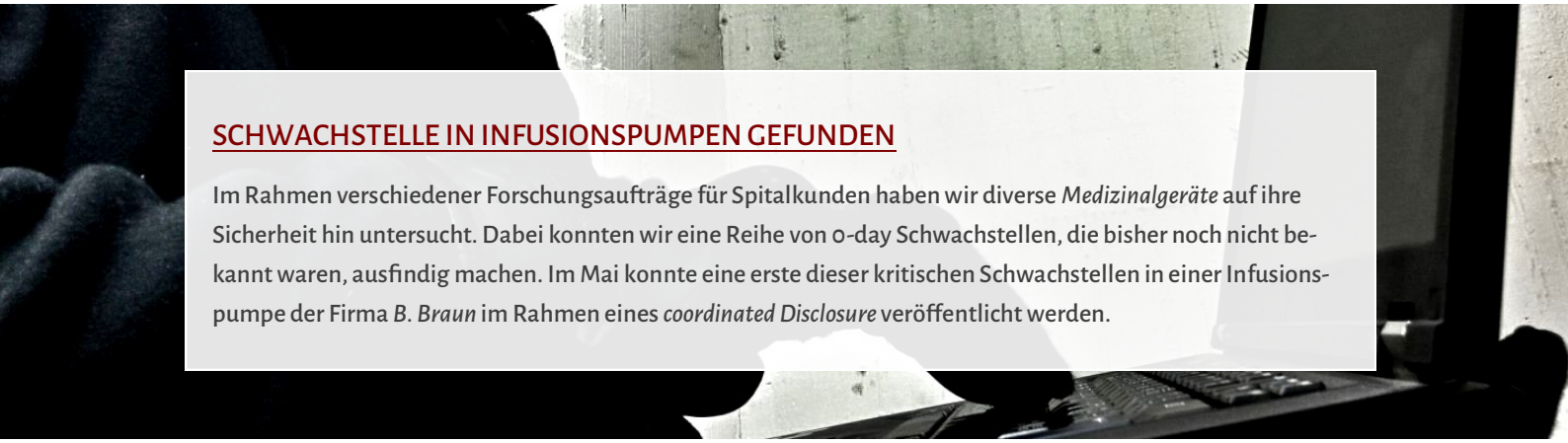
Bildquelle: https://flic.kr/p/8Nmkon

scip AG
Badenerstrasse 623
8048 Zürich
Switzerland

+41 44 404 13 13
https://www.scip.ch

NEWS

WAS IST BEI UNS PASSIERT?

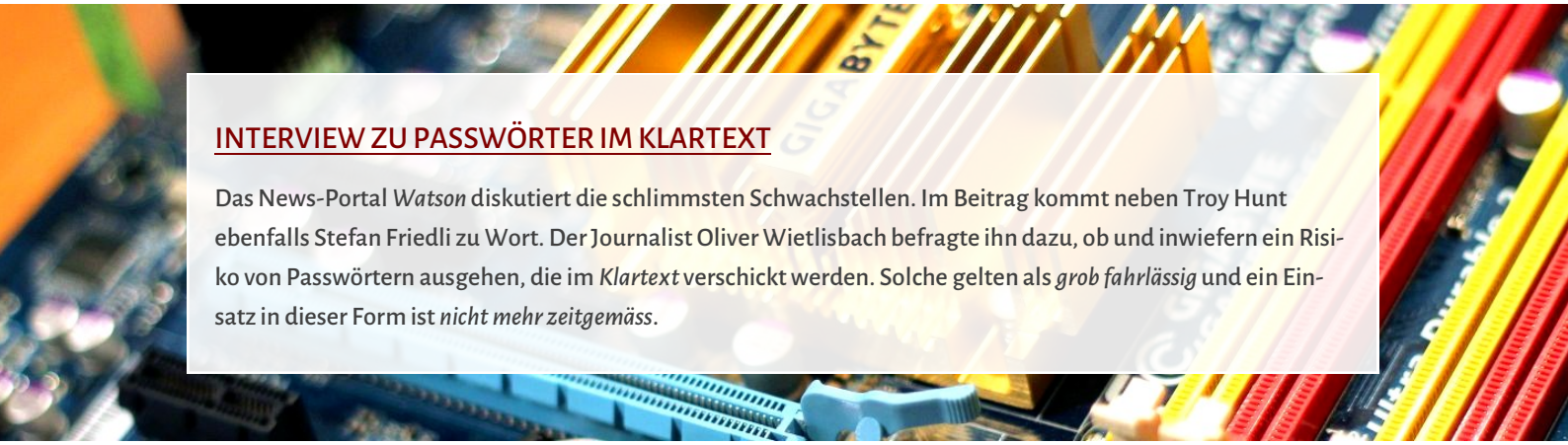


SCHWACHSTELLE IN INFUSIONSPUMPEN GEFUNDEN

Im Rahmen verschiedener Forschungsaufträge für Spitalkunden haben wir diverse *Medizinalgeräte* auf ihre Sicherheit hin untersucht. Dabei konnten wir eine Reihe von 0-day Schwachstellen, die bisher noch nicht bekannt waren, ausfindig machen. Im Mai konnte eine erste dieser kritischen Schwachstellen in einer Infusionspumpe der Firma *B. Braun* im Rahmen eines *coordinated Disclosure* veröffentlicht werden.

VORTRAG ZU MEDICAL DEVICE SECURITY IN GENF

Vom 12. bis 14. Juni fand in Genf eine Tagung der *Foundation Brocher*, die Forschung im Bereich *Humanistik* und *Gesellschaft* vorantreibt, statt. Am Event mit dem Titel *Cybersecurity Challenges in Healthcare – Ethical, Legal and Social Aspects* war Marc Ruef zugegen und hielt einen Vortrag zur Sicherheit von *Medizinalgeräten*. Dabei wurden unsere aktuellen Forschungsresultate aufgezeigt.



INTERVIEW ZU PASSWÖRTER IM KLARTEXT

Das News-Portal *Watson* diskutiert die schlimmsten Schwachstellen. Im Beitrag kommt neben Troy Hunt ebenfalls Stefan Friedli zu Wort. Der Journalist Oliver Wietlisbach befragte ihn dazu, ob und inwiefern ein Risiko von Passwörtern ausgehen, die im *Klartext* verschickt werden. Solche gelten als *grob fahrlässig* und ein Einsatz in dieser Form ist *nicht mehr zeitgemäss*.

Weitere News zu unserer Firma finden Sie auf unserer Webseite.

SCIP BUCHREIHE

UNSER AKTUELLES BUCH

Heute, mehr als je zuvor, stehen *Cyberkriminalität* und *kritische Infrastrukturelemente* im Fokus des öffentlichen Interesses. Das *Internet der Dinge*, versteckte *Marktplätze für illegale Waren*, aber auch der Diskurs über die grundsätzliche Bedeutung von *Cybersecurity* für die moderne Gesellschaft – das alles sind Themen, mit denen sich die Mitarbeitenden der scip AG im vergangenen Jahr beschäftigt und in diesem Buch zusammengefasst haben.

Trotz aller Veränderung: Auch in der achten Ausgabe mischen sich altbekannte Themenkomplexe wie *Hardening*, *Verschlüsselung* und *organisatorische Fragen* der Informationssicherheit unter die zahlreichen zeitgenössischen Themen. Und so bietet auch diese Ausgabe, wie gewohnt, einen Einblick in das weite Tätigkeitsfeld der scip AG und ihrer Mitarbeitenden.

Mit einem exklusiven Vorwort von Ivan Büchi, Head of Digital Office bei der Glarner Kantonalbank.

Weitere Informationen auf unserer Webseite.

ISBN 978-3-9524389-4-7 [de]
ISBN 978-3-9524389-5-4 [en]

DAS ERREICHEN VON SICHERHEIT IST BELOHNUNG

FLAVIO GERBINO

ASPEKTE VON CYBERCRIME CYBER– UND WIRTSCHAFTSKRIMINALITÄT

Cyber-Kriminalität, Computer- und neue Wirtschaftskriminalität sowie Fraud sind zu Modewörtern im Kontext der Informationssicherheit avanciert. Dies liegt einerseits an der technischen Entwicklung und steigenden Abhängigkeit der Organisationen von der IT und ist natürlich auch der intensivierten Vernetzung und Digitalisierung geschuldet. Welche ebenfalls dazu beitragen, dass wir uns mit einer zunehmenden Anzahl von Sicherheitsvorfällen, kriminellen Handlungen, moderneren, klügeren Attacken und systematischeren, erfolgreicheren Angriffsmethoden konfrontiert sehen.

AUS DER PERSPEKTIVE AKTUELLER VORFÄLLE

Heute sind die Angriffe, zielgerichteter und individueller auf die Opfer zugeschnitten, langfristig geplant und strategisch und organisiert angelegt. Sie sind eine permanent Bedrohung und über Grenzen hinweg omnipräsent. Diese massgeschneiderte Computerkriminalität – die als Massenware auch im Rahmen von professionellen organisierten Angeboten als *Attack as a Service* Diensten einträglich floriert – agiert ausdauernd und pausenlos.

Betroffene Organisationen sind stark herausgefordert und haben nur begrenzte Möglichkeiten, sich präventiv gegen solche neuartigen Angriffe zu schützen (wenn auch nur aus zeitlichen Gründen – denn das Einspielen von Sicherheits-Patches, wird immer noch vernachlässigt und erfordert zu viel Zeit). Ein angemessenes und effektives System an Sicherheitsmassnahmen und Kontrollen könnte es ermöglichen, sich gegen die bekannten und allenfalls die potenziell bzw. wahrscheinlichen Attacken zu schützen.

D.h. dass das in Hinblick auf die akute Bedrohungslage die detektiven und reaktiven Kontrollarten immer mehr an Bedeutung gewinnen sollten. Sie ermöglichen es den Unternehmen, im Falle eines Angriffs schnell und effektiv zu reagieren und den Schaden für das Geschäft einzudämmen und zu mindern, oder im Idealfall sogar zu vermeiden.

Von der beschriebenen Signatur war auch der letzte aktuelle Vorfall WannaCry gekennzeichnet: In der NZZ am Sonntag vom 21.05.2017 konnte man Folgendes dazu lesen:

> *Zweite Welle der Cyber-Attacke: Im Schatten der Erpresser-Software Wanna Cry haben Kriminelle Hunderttausende Computer mit einem diskreten, aber für sie weit lukrativeren Käfer infiziert: Adylkuzz. Während die Erpresser-Software «Wanna Cry» weltweit für Schlagzeilen sorgt, verbreitet sich ein zweiter Computerwurm still und leise: Adylkuzz. «Dieser Angriff ist gefährlicher als ‹Wanna Cry›, weil er im Hintergrund erfolgt und vielen Betroffenen gar nicht bewusst ist.» Darum erreiche er auch viel weniger Beachtung.*

Doch es gibt einen parallelen Handlungsstrang: Während die ganze Welt über *Wanna Cry* redet, macht sich still und leise ein weiterer Käfer breit, der auf die gleiche Art und Weise in Computer gelangt: Adylkuzz. Dieser Parasit verhält sich unauffällig und stellt keine Forderung an seine Wirte. Dafür missbraucht er deren Rechenleistung zur Herstellung einer anderen Kryptowährung namens Monero.

INTERNE BEDROHUNG ALS TREIBER

Man darf nicht vergessen, dass Unternehmen im Kontext von Fraud, Cybercrime und Wirtschaftskriminalität dabei nicht nur von aussen (extern) in From von Hacking, DDoS, Malware, Ransomware, e-Fraud etc., sondern auch durch die eigenen Mitarbeitenden (intern) gegenüber wirtschaftskriminellen Handlungen gefährdet sind. Wertewandel, zunehmende Individualisierung der Mitarbeitenden, abnehmende Loyalität gegenüber einem immer stärker fordernden Arbeitgeber, komplexe, spezialisierte Produkte und komplizenhafte Netzwerke sind Faktoren, welche die Kriminalität von innen stark begünstigen können, wie auch der individuelle Wunsch nach rascher Bereicherung.

Es ist natürlich, dass wenn hier Mitarbeitende erwähnt werden, auch das Management mit gemeint ist – denn gerade dieses scheint sich besonders oft mit internem Fraud zu verschulden. Vergleiche dazu: NZZ und KPMG Fraud Barometer für das letzte Jahr:

> *Bei der Wirtschaftskriminalität stellen – wenig überraschend – Führungskräfte aufgrund ihrer internen Stellung und ihres Handlungsspielraums in den Unternehmen die grösste Gefahr dar: So war das Management in 58% aller Fälle alleine für die Taten verantwortlich; und in weiteren 21% der Fälle machten Führungskräfte mit Angestellten gemeinsame Sache.*

Hier könnte man auch den Cyberraum als Erklärungsversuch hernehmen, um ein Motiv für den zunehmenden Betrug herzuleiten (Quelle: Stellenweise Auszug aus einem Interview mit dem bekannten Philosophen Peter Sloterdijk im Tagesanzeiger):

> *Heute sind die Vergleiche untereinander durch das Internet [vgl. Facebook, Twitter, Instagram, Snapchat etc.] virulenter geworden, man vergleicht sich direkt mit dem Bevorzugten, [gerade das Internet ermöglicht es in dieser Hinsicht jede soziale Immunabwehr aufzulösen], die schlechter gestellten treten in eine verzehrende Konkurrenz mit den Bessergestellten. Das Spektrum an Aufstiegschancen mag sich in der Moderne zwar vervielfacht haben. Aber eben deswegen produziert die moderne Gesellschaft für so viele ein Verlierergefühl: Wenn es zahllose Chancen gibt und man hat keine nutzen können, dann ist das Verlierergefühl umso bitterer [und die Motivation zu betrügen vielleicht umso grösser].*

Gerade der Finanzdienstleistungssektor scheint global der am stärksten von interner Mitarbeiterkriminalität betroffene Sektor zu sein. Betrug von innen und die in diesem Zusammenhang etablierten Compliance Regeln sowie Vorgaben werden gerade in der letzten Zeit wieder – besonders im stark regulierten Finanzdienstleistungsbereich – intensiv diskutiert und verschärft.

Die mit Wirtschafts- und Cyberkriminalität, Korruption etc. verwandten Regeln zum Schutz von Unternehmenswerten haben sich in den letzten Jahren vervielfacht. Tendenz stetig steigend. Strafverfolgung und Haftung sind inzwischen grenzüberschreitend aktiv, man verschafft sich systematisch Einblick in das digitale Innenleben von Organisationen und Unternehmen.

BEWUSSTSEIN VORHANDEN, WILLEN ZUR AKTION FEHLT

Ganz generell kann beobachtet werden, dass Sicherheit von vielen als hohes Gut in vielen Lebensbereichen hervorgehoben wird, aber die dazu angebotenen Mittel nicht angemessen genutzt werden. Insbesondere umso weniger, wenn Risiken vorgebeugt werden soll, die man selbst noch nicht erfahren hat; diese Vorbeugung aber mit Aufwand in Form von Geld, Zeit oder der Änderung gewohnter Verhaltensweisen verbunden ist. Bei Unternehmen ist dies erkennbar, dass wenn diese erstmalig oder mit neueren Betrugsformen konfrontiert sind, sie sich erst mit der Realität auseinandersetzen, obowhl sie schon zuvor bestens darüber informiert waren, dass sie von derartigen Risiken betroffen sind.

- Durch den wirtschaftlichen Druck sich permanent anzupassen, gehören Veränderungen in und an der Organisation zum Geschäftsalltag (Merger & Acquisitions, Restrukturierung, Personalabbau etc.). Dies kann zu einer Schwächung der existierenden Sicherheitsvorkehrungen führen, die von Betrügern systematisch ausgenutzt wird.

- Unternehmen kennen zwar mögliche Betrugsprobleme, sind sich häufig aber nicht der Komplexität und Vielschichtigkeit der Betrugsrisiken bewusst, denen ihre Organisationen ausgesetzt ist. Dabei fehlt die Reflexion über die Angemessenheit der existierenden Controls genauso wie auch die Ermittlung der tatsächlichen Exposition gegenüber diesen Risiken.

- Zu schwacher präventiver Schutz begünstigt ebenfalls Betrugsdelikte. Ein Mangel an deduktiven, nachträglich aufdeckenden Massnahmen (Logging, Monitoring, SIEM etc.) kann dazu führen, dass interne Betrugsdelikte erst nach langer Zeit ans Tageslicht gelangen – oder gar nie.

- Unkenntnis der Mitarbeitenden, was zu tun ist, wenn sie einen Betrug vermuten oder entdecken. Dadurch kann es aus Angst und Unwissenheit dazu kommen, dass ein potentieller oder realer Betrug nicht gemeldet wird oder darauf nicht angemessen reagiert wird. Der Ausspruch von Benjamin Frenklin An ounce of prevention is worth a pound of cure scheint hier besonders zutreffend zu sein. Oder einfach gesagt Prevention is better than curing – Prävention ist besser als heilen.

WANN WIRD AUS EINER HANDLUNG EINE STRAFTAT?

Mit zunehmender Digitalisierung und Automatisierung stehen die IT-Systeme verstärkt im Fokus der Täter. Schwachstellen in den internen Kontrollen können durch interne oder externe Angreifer missbräuchlich genutzt und so Daten in grossen Mengen entwendet oder zweckentfremdet werden. Neben dem Begriff der Computerkriminalität gewinnt daher auch zunehmend die *Cyberkriminalität* an Bedeutung, die hier dadurch unterschieden ist, dass *Cybercrime* als kriminelle Aktivität bezeichnet, welche explizit mithilfe des Internets ausgeführt wird.

Kriterien für die Kriminalität einer Cyberaktivität:

- strafrechtlich relevant

- zum Nachteil des Unternehmens

- Vorsätzlich durchgeführte Handlungen der Mitarbeiter, der gesetzlichen Vertreter, der Mitglieder der Aufsichtsorgane oder Dritter (im Falle von Betrug von innen)

Dabei wird normalerweise angenommen, dass durch die Handlung ein ungerechtfertigter oder rechtswidriger Vorteil erlangt wird.

ROLLE DER IT- UND INFORMATIONSSICHERHEIT

Die ursprüngliche – und weiterhin wichtige – Aufgabe der Vertreter der Informationssicherheit ist ihr Einsatz bei internen Ermittlungen, Prüfungen, Audits, Untersuchungen oder Investigationen etc.

Aus Sicht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umfasst eine Cybercrime-Untersuchung als Aufgabe der Informationssicherheit:

> *eine methodisch vorgenommene Datenanalyse auf Datenträgern und in den Computernetzen zur Aufklärung von Verdachtsmomenten bzw. des Verdachts auf dolose Handlungen.*

Im Rahmen von Data Mining, Data Matching, Datenanalyse, Umfeldanalyse sowie Analyse der internen Kontrollen sollten folgende Informationen gewonnen werden:

- Beschreibung des Betrugsfalls nach Zeit und Ort
- Konkrete Beschreibung der Art des Vorfalls
- Kontrollen- und Schwachstellenanalyse
- Informationen über die am Vorfall Beteiligten, Identifizierung von Tätern
- Ermittlung des Schadensumfangs (Wert, Ausmass) und möglicher Folgeschäden

Die Rolle Informationssicherheitsvertreter:

- **Informationsgewinnung**: relevante Informationen gewinnen
- **Informationsauswertung**: Informationen analysieren und bewerten
- **Bereitstellung der Ergebnisse**: Ergebnisse und Beweise den Ermittlern bzw. Prüfern bereitstellen
- **Aufarbeitung**: Informationen zielgruppengerecht aufarbeiten, damit die an den Prüfungen und Ermittlungen Beteiligten die Daten verstehen und korrekt in ihre Denkprozesse integrieren können

Und weiter:

- Durchführung von diversen internen Befragungen (Interviews)
- gerichtsverwertbare Beweissicherung (Zeitstempel, Verschlüsselung, qualifizierte Signatur etc.)
- digitale Beweissicherung (E-Mails, Festplatten, USB-Sticks, Cloud etc.)
- Analyse und Darstellung von Prozessabläufen
- Feststellung der Schadenshöhe zur Durchsetzung von Schadensersatzleistungen
- Mitarbeit beim Festhalten der Ergebnisse im Reporting

Obwohl die Cyberkriminalität vorrangig als Domäne der international agierenden, geographisch verteilten organisierten Gruppen gilt, sind an den kostspieligsten bekannten Attacken sehr oft Insider beteiligt gewesen.

Typische Beiträge an Cyber-Attacken durch interne Mitarbeiter sind daher:

- Lokalisierung von Vermögensgegenständen (Asset Tracing)
- Analyse von Geldflüssen (Follow the Money)
- Rekonstruktion von Transaktionen
- Preisgabe von Insiderwissen

MÖGLICHE ANSATZPUNKTE

Um dem Cybercrime und Fraud in allen Ausprägungen entgegenzuwirken, bedarf es einer strukturierten Vorgehensweise, die sich in 3 klassische Bereiche der Fraudbekämpfung gliedert: Prävention, Aufdeckung und Reaktion.

Oft lassen sich Aktivitäten gut in bestehende Organisationsstrukturen integrieren (prädestiniert sind Informationsecurity- und Compliance-Management), bereits vorhandene Schnittstellen können genutzt werden, um Synergeieffekte zu erzielen. Voraussetzungen hierfür sind:

- Bereitschaft Ressourcen für die Organisation von Anti-Fraud und Anti-Cybercrime Aktivitäten freizugeben
- Entwicklung und Gestaltung Regeln, Richtlinien und Arbeitsanweisungen
- Implementierung von Monitoring
- Konzeption und Durchführung von Risikoanalysen mit konkreten Szenarien
- Durchführung von Schulungen

Innerhalb der 3 klassischen Bereiche der Fraudbekämpfung sind folgende Themen zu behandeln:

- **Verhindern / Prävention**: Weitestgehende Vermeidung von konkreten Risikoszenarien: Hierzu zählen Regelwerke (zum Beispiel Anti-Fraud -Richtlinie, Code of Conduct, Umgang mit Interessenkonflikten und Zuwendungen, Schulungen, Zuverlässigkeitsprüfungen bei Mitarbeitenden, Due Diligence (Front-Prozesse), Gefährdungs- und Risikoanalysen).
- **Aufdecken / Detektion**: Anhand definierter Schwellenwerte mit dem Ziel die Dauer des Fraudfensters zu verkürzen: Monitoring-Prozesse und Tools, Hinweisgebersystem, Gefährdungs- und Risikoanalysen.
- **Aufarbeiten**: Fälle, die einen definierten Schwellenwert übersteigen müssen aufgearbeitet und sanktioniert werden. Zu diesem Schritt zählt auch das regelmässige identifizieren von Cybercrime und Fraud Risiken, um die darauf angemessene Reaktion verbessern zu können: Kommunikationskonzepte (intern und extern), Notfallpläne, Anreizprogramme, Sanktionssystem, Lessons learned-Prozess, Reporting.

Flavio Gerbino

FAZIT

Um sich so gut wie möglich gegen Fraud und Cybercrime zu schützen, muss ein besonderes Augenmerk auf folgende Punkte gelegt werden:

- Konsequente Anwendung von Data Analytics, Monitoring, Logging bei Key-Systemen und Schnittstellen sowie volle Kontrolle über Datenanalyse innerhalb der gesamten relevanten Bereiche.

- Planung und Durchführung szenarienbasierter, interaktiver Sessions zur Beurteilung von Betrugsrisiken im Kontext der Branche und des Unternehmens. Risiken müssen so spezifisch wie möglich identifiziert und quantifiziert werden und das Management muss über die für die Organisation bestehenden Risiken und die zu ergreifenden Massnahmen aufgeklärt und geschult werden.

- Etablierung von Key-Controls in bedeutenden Geschäftsbereichen und sicherstellen, dass angemessene präventive und deduktive Massnahemen eingerichtet wurden, einschliesslich der kontinuierlichen

- Überwachung der Wirksamkeit sowie weitere automatisierte technische Lösungen zur Unterstützung: Automatisierte Auswertungstools gewinnen bei der Prävention, Detektion und Reaktion, insbesondere in Hinblick auf die steigende Computer- und Cyber-Kriminalität, zunehmend an Bedeutung. Nicht zuletzt aufgrund ihrer Effizienz (Big Data), Versatilität und dem Potential Kosten für die analytischen, forensischen oder deduktiven Analysen kosten zu senken, die sonst oft manuell und mit erheblichem Aufwand von Spezialisten durchgeführt werden müsste.

- Aufbau von koordinierten, zielgerichteten Strategien, Systemen, Richtlinien, Verfahren und Prozesse zur aktiven Bekämpfung von Betrug.

- Generelle Awareness und konkrete Schulungen für Betrugsdelikte auf allen Stufen (Verwaltungsrat, Management, Audit Committees, Geschäftsleitung, Mitarbeitende, und andere identifizierte Key-Employees).

next gen vulnerability intelligence

VulDB

Seien Sie schneller als Ihre Angreifer

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

MARC RUEF

ANTI-FRAUD BEI ONLINE-DIENSTEN

Banken, Kreditkartenaussteller und Online-Händler sind gleichermassen mit dem Problem des Betrugs konfrontiert. Dieser Artikel bespricht, wie anhand des Verhaltens von Betrügern bzw. den durch sie zugeführten Zugriffen böswillige Aktivitäten erkannt und auf diese reagiert werden kann.

DER NORMALE BENUTZER

Man kann sagen, dass es soetwas wie den normalen Benutzer gibt. Darunter versteht man alle Benutzer, die sich im bzw. nahe am durchschnittlichen Verhalten bewegen. Zum Beispiel sind der grösste Teil der Facebook-Benutzer zwischen 25 und 34 Jahre alt (29.7%), bestehen aus weiblichen Benutzern (76%) und benutzen die Seite im Schnitt 20 Minuten. Falls Sie diese drei Eigenschaften für Sie vereinen, handelt es sich bei Ihnen um den durchschnittlichen Facebook-Benutzer.

Solche Statistiken lassen sich für sämtliche Angebote, Dienste und Nutzungsbereiche erstellen. In manchen Fällen sehen die Resultate verschiedener Plattformen ähnlich aus, in anderen gibt es ganz offensichtliche soziodemografische und/oder technische Abweichungen.

Um betrügerisches Verhalten erkennen zu können, muss als erstes das normale Verhalten identifiziert werden. Auf technischer Ebene sind dies zum Beispiel:

- Webbrowser (Hersteller, Produkt, Version, Plattform)
- Spracheinstellungen (z.B. Accept-Language im Header der HTTP-Anfrage)
- Geolokalisierung

Abweichungen von der ermittelten Normalität können sodann Hinweise auf betrügerisches Verhalten sein. Bei der Einführung einer ersten Implementierung sollte man sich am Durchschnitt aller Benutzer orientieren. Professionelle Lösungen im Finanzbereich vergleichen mit dem normalen Verhalten des spezifischen Benutzers, der Benutzer im gleichen Postleitzahlenbereich und der Benutzer in der gleichen geografischen Sprachregion. Andere Gruppierungen (z.B. eingesetzter Webbrowser) sind ebenfalls denkbar.

STRAFPUNKTE BEI ABWEICHUNGEN

Der empfohlene Ansatz sieht nicht vor, dass sämtliche Abweichungen sofort als betrügerisches Verhalten verstanden und sanktioniert werden sollen. Viel mehr soll durch das Zusammenführen verschiedener Indizien eine Beweislage geschaffen werden, auf der Basis derer eine nachvollziehbare Entscheidung getroffen werden kann.

Zu diesem Zweck sollen Strafpunkte für einzelne Abweichungen definiert werden. Die Abweichungen sollten aufgelistet und in verschiedene Kategorien an Schweregrad aufgeteilt werden. Es ist unnötig, für einen Übergriff 51 Punkte und für einen anderen 59 Punkte vergeben zu können. Stattdessen sollte man möglichst mit einstelligen Punkten, in diesem Fall 5 und 6, arbeiten. Dies vereinfacht das System enorm und erhöht den Überblick.

Um False-Positives zu vermeiden, sollte bei der Zunahme der Schwere eines Verstosses mit überproportionalen Abstufungen gearbeitet werden. Bewährt haben sich exponentielle Erhöhungen der Form 1, 2, 4, 8 und 16. Es ist für einen Kunden viel schwieriger, versehentlich im Maximum zu landen, weder wenn eine Skala von 1, 2, … 5 eingesetzt werden würde.

Die Anzahl der Abstufungen sollte 3, 4, 5 oder 6 Möglichkeiten zulassen. Weniger 3 als schränken bei der Punktevergabe ein. Und bei mehr Möglichkeiten wird wiederum die Komplexität und Nachvollziehbarkeit negativ beeinträchtigt.

Die Metrik ist immer individuell auszulegen und muss im Rahmen der Erarbeitung des Modells iterariv erarbeitet werden.

Beispiel Schweizer Online-Händler

Im folgenden Beispiel soll aufgezeigt werden, wie die Abstufung für die Geolokalisierung bei einem Schweizer Online-Händler, der keinen internationalen Versand vorsieht, stattfinden kann:

Client-IP-Adresse:

- IP-Adresse ausserhalb CH → 1
- IP-Adresse ausserhalb DACH → 2
- IP-Adresse ausserhalb EU → 4
- IP-Adresse ausserhalb Europa → 6
- IP-Adresse in Ländern mit hoher Cybercrime-Rate (z.B. Russland, China) → 8
- IP-Adresse von bekanntem VPN-Dienst oder Tor Exit Node → 8

Webbrowser:

- User-Agent kein zeitgenössischer Browser → 4
- Leerer User-Agent String → 8

Versandadresse:

- Versand an bekannten Benutzer mit offenen Rechnungen → 2
- Versand an bekannten Benutzer mit bekannten Betreibungen → 4
- Versand an neuen Benutzer ohne bisherige Bestellungen → 4
- Versand an nicht existente Adresse → 6

Zeitgestützte Abweichungen

Eine besondere Klasse von Abweichungen ist jenachdem auf der Zeitachse zu beobachten. Es gibt typische Pausen, die normale Benutzer zwischen Aktivitäten einbringen. Zum Beispiel dauert es x Sekunden, bis nach dem Laden der Login-Seite die entsprechenden Credentials eingegeben wurden. Ist diese Pause speziell kurz oder lang, kann dies wiederum auf ein verdächtiges Verhalten hinweisen. Zum Beispiel lassen sich so Automatisierungen (z.B. Bruteforce-Attacken) sehr einfach erkennen. Ein Angreifer müsste in diesem Fall zufällige aber realistisch wirkende Verzögerungen einbringen, um dadurch nicht erkannt werden zu können.

Zeitgestützte Abweichungen orientieren sich immer am Zeitpunkt zweier unterschiedlicher Aktionen. Diese Aktionen müssen dabei nicht direkt nacheinander erfolgen. Die Eingabe der Credentials und das Abschicken des Login-Formulars folgt in der Regel aufeinander. Man kann aber auch stattdessen die Zeit zwischen der Eingabe des Benutzernamens und der ersten Ausgeführten Transaktion im Online-Banking beobachten. Jenachdem deuten Abweichungen auf ein zielgerichtetes Plündern von Konten hin.

Wie bei allen Abweichungen sollen auch die zeitbasierten Abweichungen mit Strafpunkten belegt werden. Hier folgt man dem gleichen Schema, das für die Taxierung der eigentlichen Aktionen genutzt wird. Als Aktion ist hier jedoch der zeitliche Ablauf zweier Aktionen zu verstehen.

THRESHOLDS FÜR AKTIONEN

Beim Erreichen eines vordefinierten Thresholds kann eine Aktion ausgelöst werden. Diese können eine ganze Bandbreite von passiven oder aktiven Aktionen umfassen. Zum Beispiel:

- Warn-/Fehlermeldung
- Erweitertes Logging
- Informieren bestimmter Stellen
- Verlangsamung der Verarbeitung
- Manuelle Prüfung erforderlich
- Zusätzliche Identifikation erforderlich
- Zusätzliche Authentisierung erforderlich
- Einschränken von Zugriffsmöglichkeiten
- Unterbinden sämtlicher Zugriffe

Es gilt also zu definieren, ab welcher Summe von Strafpunkten welche Aktion ausgelöst wird. Die Schwierigkeit besteht hier darin, den goldenen Mittelweg zu finden. Bei False-Negatives werden illegitime Zugriffe nicht erkannt bzw. nicht darauf reagiert. Und bei False-Positives werden Restriktionen zu rigoros angewendet und damit legitime Zugriffe unnötig erschwert. Beides gilt es zu verhindern.

```
if(password_verify($_POST['password'], $row['password'])){
   echo 'You are authenticated!';
}else{
   $_SESSION['penalty'] = $_SESSION['penalty'] + 1;
   echo 'Authentication failed.';
}
```

Beispiel fehlerhafte Logins

Ein leicht nachvollziehbares Beispiel liefert das Verhalten bei fehlerhaften Login-Versuchen. Der Einfachheit halber gehen wir davon aus, dass jeder fehlerhafte Login-Versuch den Strafpunktebestand um 1 erhöht.

1. (3) Benachrichtigung des Kontoinhabers über verdächtige Aktivitäten. Zurücksetzen des Passworts offerieren, falls es vergessen wurde.

2. (5) Verlangsamen der Datenverarbeitung um 1-3 Sekunden, um Bruteforce-Angriffe stark zu verlangsamen.

3. (10) Login ist gar nicht mehr möglich. Der Benutzer wird aber nicht darauf hingewiesen, so dass Bruteforce-Zugriffe ins "Leere" laufen. Selbst die Eingabe der richtigen Login-Daten würde nicht zu einem Login führen.

4. (25) Sperren der Quell-IP-Adresse für sämtliche Login-Versuche für alle Benutzerkonten für 15 Minuten, um breitflächige Bruteforce-Attacken einzuschränken.

Hierbei ist zu sehen, wie ein Innen-nach-Aussen Ansatz gewählt wurde: Die Bestrafung wird zuerst möglichst eng gefasst (nur punktuelle Information) und dann immer mehr ausgeweitet (langsamer und dann einschränken). Dadurch können Kollateralschäden verhindert oder wenigstens hinausgezögert werden.

Ansatz zur Ermittlung von Abstufungen

Der Aspekt bei dem hier diskutierten Ansatz, der den meisten Kunden die grössten Probleme bereiten, ist das Entwickeln einer Metrik samt ihrer Abstufungen. In Bezug auf fehlerhafte Login-Versuche scheint dies noch einfach zu sein. Komplizierter wird es aber, wenn man Transaktionen nach einem erfolgreichen Login überwachen will.

```
if($_SESSION['penalty'] >= 3){
   mailuser();
}elseif($_SESSION['penalty'] >= 5){
   slowdown();
}elseif($_SESSION['penalty'] >= 10){
   disablelogin();
}
```

Hierbei gilt es in Szenarien zu denken. Die für die diskutierten Szenarien generierten Punkte sind entsprechend zu sanktionieren. Wenn uzm Beispiel ein Betrüger einen Account übernommen hat, um eine Bestellung an eine nicht existierende Adresse zu schicken, den Zugriff via VPN durchsetzt und den diesen automatisiert hat (es wird kein User-Agent String mitgeschickt), ergibt dies 22 Punkte. Anhand der unten definierten Thresholds würde dies das Einschränken der Zugriffsmöglichkeiten nach sich ziehen:

- 4 → Warn-/Fehlermeldung
- 6 → Erweitertes Logging
- 12 → Verlangsamung der Verarbeitung
- 16 → Informieren bestimmter Stellen
- 16 → Zusätzliche Identifikation erforderlich
- 18 → Zusätzliche Authentisierung erforderlich
- 20 → Manuelle Prüfung erforderlich
- 22 → Einschränken von Zugriffsmöglichkeiten
- 25 → Unterbinden sämtlicher Zugriffe

Während der Diskussion der Szenarien kann auffallen, dass einzelne Verstösse nicht offensichtlich genug mit Strafpunkten versehen sind. Dass sich also kleinere Verstösse nicht früh genug erkennen oder sich nicht von groben Verstössen unterscheiden lassen. In diesem Fall muss man die grundlegenden Strafpunkte neu vergeben. Es erfordert viel Zeit und Diskussionen, um ein nachhaltiges Model entwickeln zu können, das zuverlässig arbeiten kann.

MIT SIMULATIONEN ARBEITEN

Die Schwierigkeit besteht darin, ein zuverlässiges Modell zu erarbeiten. Zu diesem Zweck ist eine umfassende Auswertung des legitimen Verhaltens erforderlich. Hierfür müssen unter Umständen mehrere Monate von Benutzerzugriffen ausgewertet und gruppiert werden. Die grosse Datenlage macht diese Arbeit komplex und aufwendig.

Dennoch oder gerade deswegen empfehlen wir einen simulationsbasierten Ansatz. Das Modell wird als Simulation zur Verfügung gestellt, in der die bisher angefallenen Daten eingebracht werden können. Durch das Parametrisieren der Events, Thresholds und Actions können statistische Aussagen zur Zuverlässigkeit (False-Positives und False-Negatives) einzelner Einstellungsvarianten getroffen werden.

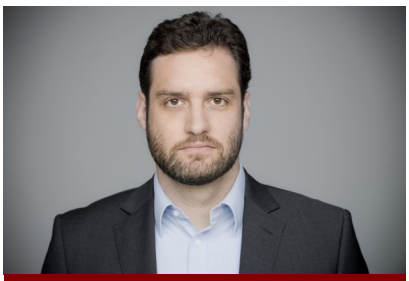
Das Erreichen eines perfekten Modells ist eigentlich niemals möglich. Eine Gewisse Abweichung des Optimums muss immer in Kauf genommen werden. Die Simulation hilft dabei, diese Abweichung erkennen und akzeptieren zu können. Auch dadurch vielleicht 2% der Betrugsfälle trotzdem nicht erkannt und verhindert werden können, stellt dies eine Verbesserung von 98% dar.

ZUSAMMENFASSUNG

Betrug in Online-Diensten ist kein neues Phänomen. Stattdessen hat hierbei eine regelrechte Professionalisierung stattgefunden. Diese zu bekämpfen ist wichtig, um gewisse Dienste zuverlässig und wirtschaftlich halten zu können.

Zu diesem Zweck lohnt sich der Einsatz einer Anomalieerkennung. Zuerst muss das normale Verhalten ermittelt werden, um Abweichungen erkennen und richtig taxieren zu können. Durch das Vergeben von Strafpunkten werden irgendwann vordefinierte Thresholds erreicht, wodurch punktuelle Aktionen ausgelöst werden können. Dadurch können Angriff erschwert oder gänzlich abgewehrt werden.

Eine Simulation hilft dabei, ein optimales Modell zu entwickeln. Es ist wichtig dabei zu bedenken, dass man sich in der Regel dem Optimum nur annähern, dieses jedoch nie erreichen kann. Eine Verbesserung ist aber in jedem Fall möglich und sollte dementsprechend auch angestrebt werden.



Marc Ruef

)SCIP(

AUCH SCHÖNHEIT KENNT RISIKEN

Bildquelle: https://pixabay.com/photo-21649/

VULNERABILITY SUMMARY

AUSGEWÄHLTE SCHWACHSTELLEN DES AKTUELLEN MONATS

1

GOOGLE ANDROID BIS 7.1.2 MEDIASERVER MEDIA FILE PUFFERÜBERLAUF

https://vuldb.com/de/?id.102516

Es wurde eine kritische Schwachstelle in Google Android bis 7.1.2 ausgemacht. Hiervon betroffen ist eine unbekannte Funktion der Komponente Mediaserver. Durch das Manipulieren durch Media File kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Es sind weder technische Details noch ein Exploit zur Schwachstelle bekannt. Es muss davon ausgegangen werden, dass ein Exploit zur Zeit etwa USD $5k-$25k kostet (Preisberechnung vom 06/14/2017). Die Schwachstelle lässt sich durch das Einspielen eines Patches beheben.

2

VMWARE ESXI/WORKSTATION PRO/PLAYER/FUSION PRO/FUSION SVGA PUFFERÜBERLAUF

https://vuldb.com/de/?id.102080

Eine sehr kritische Schwachstelle wurde in VMware ESXi, Workstation Pro, Player, Fusion Pro sowie Fusion - die betroffene Version ist nicht genau spezifiziert - entdeckt. Davon betroffen ist eine unbekannte Funktion der Komponente SVGA. Es sind weder technische Details noch ein Exploit zur Schwachstelle bekannt. Es muss davon ausgegangen werden, dass ein Exploit zur Zeit etwa USD $5k-$25k kostet. Für den Vulnerability Scanner Nessus wurde ein Plugin mit der ID 99103 herausgegeben. Ein Upgrade vermag dieses Problem zu beheben.

3

MICROSOFT WINDOWS BIS SERVER 2016 SEARCH ERWEITERTE RECHTE

https://vuldb.com/de/?id.102387

Es wurde eine sehr kritische Schwachstelle in Microsoft Windows, ein Betriebssystem, gefunden. Es geht dabei um eine unbekannte Funktion der Komponente Search. Durch Beeinflussen mit einer unbekannten Eingabe kann eine erweiterte Rechte-Schwachstelle ausgenutzt werden. Der Angriff kann über das Netzwerk erfolgen. Zur Ausnutzung ist keine spezifische Authentisierung erforderlich. Der Preis als 0-Day war auf dem Schwarzmarkt etwa $100k-$500k. Die Schwachstelle lässt sich durch das Einspielen des Patches KB4022719 lösen.

4

MICROSOFT WINDOWS XP SP3/SERVER 2003 SP2 RDP ERWEITERTE RECHTE

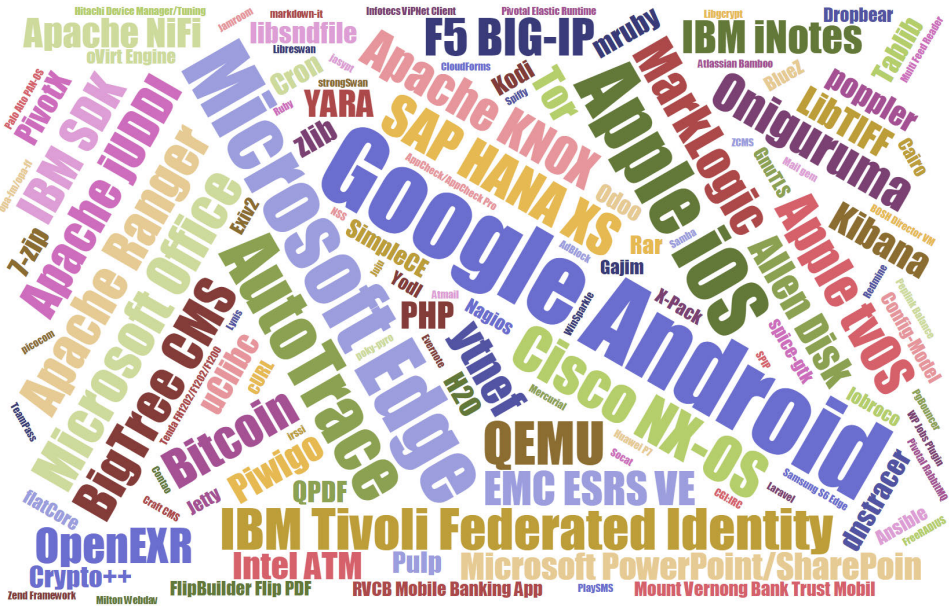
https://vuldb.com/de/?id.102511

In Microsoft Windows XP SP3/Server 2003 SP2, ein Betriebssystem, wurde eine kritische Schwachstelle entdeckt. Das betrifft die Komponente RDP. Um eine Ausnutzung durchzusetzen, muss keine spezifische Authentisierung umgesetzt werden. Technische Details sind nicht bekannt und ein Exploit zur Schwachstelle ist ebenfalls nicht vorhanden. Die Beschaffenheit der Schwachstelle lässt vermuten, dass ein Exploit momentan zu etwa USD $25k-$100k gehandelt werden wird. Die Schwachstelle lässt sich durch das Einspielen eines Patches lösen.

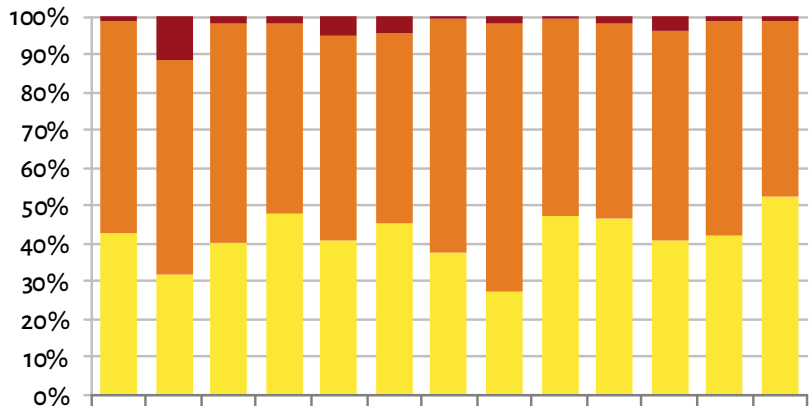
VULNERABILITY LANDSCAPE

AKTUELLE STATISTIKEN AUS UNSERER VULDB

MEISTEXPONIERTE PRODUKTE IM VERGANGENEN MONAT



VERLAUF DER RISIKEN DER VERGANGENEN 12 MONATE



	Jun 16	Jul 16	Aug 16	Sep 16	Okt 16	Nov 16	Dez 16	Jan 17	Feb 17	Mar 17	Apr 17	Mai 17	Jun 17
sehr kritisch	6	109	8	12	49	28	2	23	4	28	55	9	6
kritisch	296	550	308	437	536	346	517	1054	499	929	895	639	353
problematisch	227	309	212	409	406	313	312	407	454	834	659	478	398

Datenquelle: https://vuldb.com/de/

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

Verantwortlich für diese Ausgabe:
Stefan Friedli & 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 DIE 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 Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Switzerland

+41 44 404 13 13
www.scip.ch