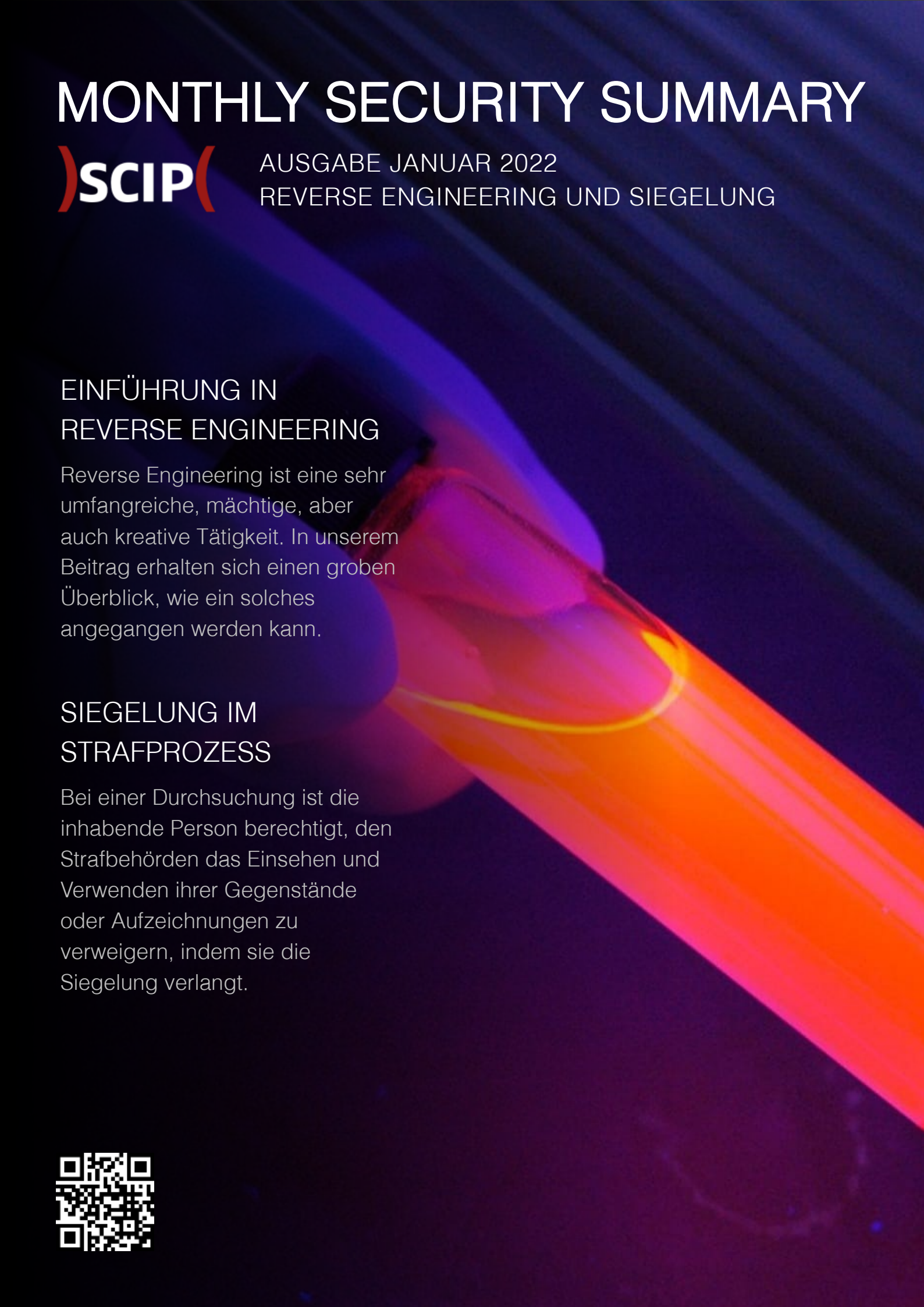
MONTHLY SECURITY SUMMARY

AUSGABE JANUAR 2022
REVERSE ENGINEERING UND SIEGELUNG



EINFÜHRUNG IN REVERSE ENGINEERING

Reverse Engineering ist eine sehr umfangreiche, mächtige, aber auch kreative Tätigkeit. In unserem Beitrag erhalten sich einen groben Überblick, wie ein solches angegangen werden kann.

SIEGELUNG IM STRAFPROZESS

Bei einer Durchsuchung ist die inhabende Person berechtigt, den Strafbehörden das Einsehen und Verwenden ihrer Gegenstände oder Aufzeichnungen zu verweigern, indem sie die Siegelung verlangt.

Januar 2022: Achtung, Supply-Chain!

Supply-Chain. Ein Begriff, der die letzten Monate dominiert und damit ins breite Bewusstsein der Gesellschaft katapultiert wurde. Produkte erfordern *Einzelteile*, die nicht selten *eingekauft statt selber produziert* werden. Falls die Lieferungen für diese Einzelteile ausbleiben, kann auch das eigentliche Produkt nicht erstellt und verkauft werden. Die Produktion kommt zum Erliegen.

In der *Cybersicherheit* hat das Thema *Supply-Chain* aber noch einen anderen wichtigen Aspekt: Die gelieferten Komponenten müssen frei von Manipulationen und Schwachstellen sein. Werden nämlich Computerchips oder Software als *Einzelteil* für eine Lösung geliefert, kann durch eine Manipulation dieser die Kompromittierung des Endprodukts durchgesetzt werden.

Hintertüren in Mikrochips oder Server-Komponenten können verheerende Konsequenzen für Hersteller und Kunden haben. Deshalb gilt sich konkrete Gedanken darüber zu machen, woher gewisse Einzelteile stammen, ob man diesen vertrauen und wie man die Sicherheit dieser prüfen kann.

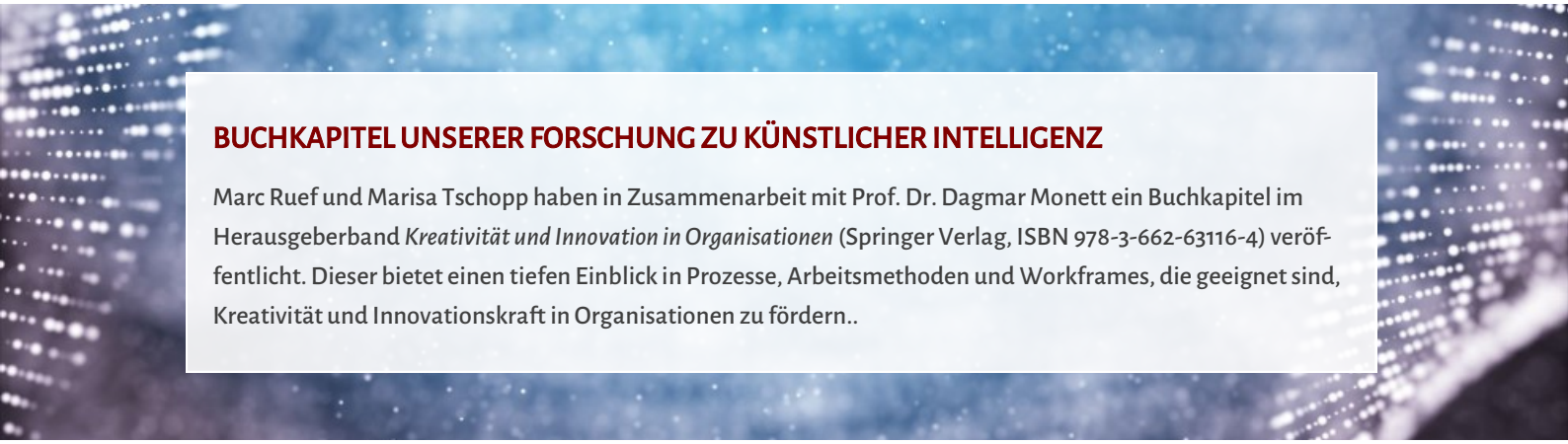
Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

FERNSEHINTERVIEW ZU DATENLECK IN DER SENDUNG PLUSMINUS

Sie Sendung *Plusminus* setzt sich mit einem *breitflächigen Datenleck* bekannter Online-Anbieter in Deutschland auseinander. In der Sendung kommt Marc Ruef zu Wort, der erklärt, wie mit solcherlei gestohlenen Daten im *Darknet* umgegangen wird, wie sie gehandelt und missbraucht werden. Der Beitrag von Julian Gräfe kann in der in der *Mediathek* und auf *YouTube* gesehen werden.



BUCHKAPITEL UNSERER FORSCHUNG ZU KÜNSTLICHER INTELLIGENZ

Marc Ruef und Marisa Tschopp haben in Zusammenarbeit mit Prof. Dr. Dagmar Monett ein Buchkapitel im Herausgeberband *Kreativität und Innovation in Organisationen* (Springer Verlag, ISBN 978-3-662-63116-4) veröffentlicht. Dieser bietet einen tiefen Einblick in Prozesse, Arbeitsmethoden und Workframes, die geeignet sind, Kreativität und Innovationskraft in Organisationen zu fördern..

EINFÜHRUNG EINES ÖFFENTLICHEN BUG BOUNTY PROGRAMMS

Cybersecurity ist uns wichtig. Aus diesem Grund haben wir ein öffentliches *Bug Bounty Programm* eingeführt. Dieses lädt Researcher ein, in unseren Services gefundene Schwachstellen zu melden. Relevante Reports werden umgehend adressiert und entsprechend vergütet. Dabei unterstützen wir den Standard *draft-foudil-securitytxt-12*, indem wir eine stets aktuelle *security.txt* bereitstellen.

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]

GENAU HINSCHAUEN LOHNT SICH

Bildquelle: https://pixabay.com/images/id-6907394/

RALPH MEIER

REVERSE ENGINEERING ALS EINSTIEG

Reverse Engineering ist eine sehr umfangreiche, mächtige, aber auch kreative Tätigkeit. Im Artikel Reverse Engineering – Erweiterte Sicherheitsüberprüfungen werden die drei verschiedenen Hauptbereiche im Reverse Engineering bereits erläutert. In diesem Artikel liegt der Fokus auf das *Disassemblieren* und *Dekompilieren* von Software.

WAS IST REVERSE ENGINEERING?

Reverse Engineering ist der *umgekehrte Vorgang* zur normalen Entwicklung eines Produkts, sprich der Prozess beginnt mit einem fertigen Produkt und man baut es in seine Einzelteile zurück. Dabei muss das Produkt nicht zwingend vollendet sein. Reverse Engineering ist nicht nur auf Software beschränkt, sondern auch im Hardwarebereich anwendbar.

Beim Auseinandernehmen eines fertigen Produkts kommt schnell der Gedanke an Kopieren beziehungsweise Imitieren eines Produkts auf. Dies ist sicher ein valider Punkt, es gibt aber eine Vielzahl weiterer Gründe für den Einsatz von Reverse Engineering.

Analyse

Das Analysieren eines eigenen Produktes macht zum Beispiel Sinn, wenn viele Knowhow-Träger das Unternehmen verlassen haben und die vorhandene Dokumentation unvollständig ist. Daher will man mit Hilfe von Reverse Engineering verlorengegangenes Wissen wieder gewinnen und sogenanntes *Redocumentation* und *Design Recovery* betreiben.

Im Hardware-Bereich können durch die Hilfe von Reverse Engineering Alternativen zu verbauten Chips in älteren Produkten oder Designs gefunden werden, um der derzeitigen Chip Knappheit ein wenig auszuweichen. Damit lässt sich teilweise auch Obsoleszenz vorbeugen, wenn ein Chiphersteller pleiteging oder benötigte Bauteile nicht mehr produziert werden.

Interfacing

Mit Interfacing ist gemeint, durch den Einsatz von Reverse Engineering *Kompatibilität zu fremden Systemen* aufzubauen. Dabei findet man heraus, wie das Drittsystem funktioniert und wie es am besten angesprochen wird. Daraus lässt sich mit genügend Er-

kenntnis eine Schnittstelle zwischen dem eigenen und dem Dritt-System erstellen.

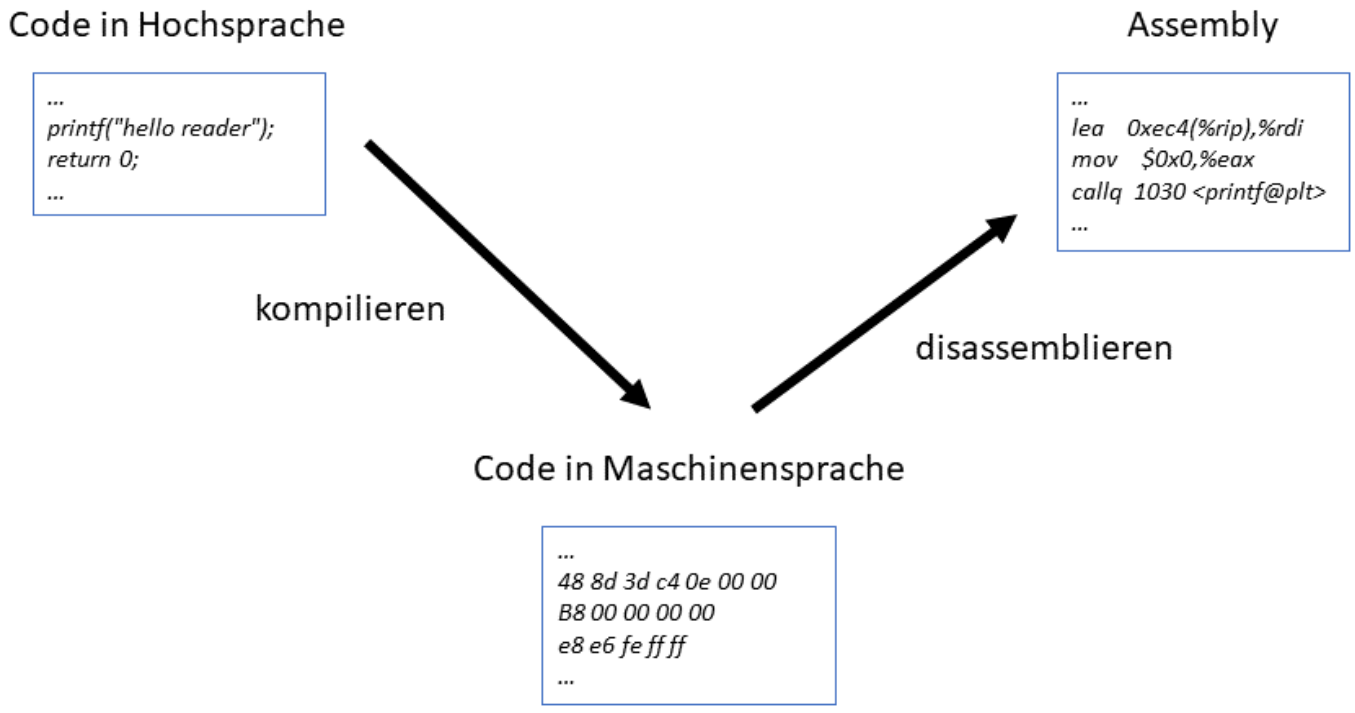
Security Analyse

In der Security Analyse werden Software und Hardware auseinandergenommen, um mögliche Angriffspunkte und Schwachstellen zu ermitteln. Diese werden dann den Hersteller gemeldet, um zukünftiges Ausnutzen davon zu vermeiden. Bei Blackbox Tests wird oft Reverse Engineering verwendet, um das Verständnis des Testobjekts erweitern zu können.

Reverse Engineering wird zudem beim *Analysieren von Malware* eingesetzt. Unter anderem um herauszufinden, wie der Schlüssel einer Ransomware erstellt wird, um verschlüsselte Daten so schnell wie möglich wiederherstellen zu können. Oder auch um herauszufinden, welches Hacker Kollektiv hinter einem Angriff steckt.

DISASSEMBLIEREN UND DEKOMPILIEREN

Beim Rückübersetzen von Software oder generell kompilierten Programmiercode gibt es zwei verschiedene Arten. Zum einen Disassemblieren, wobei *Code in Maschinensprache* in von Menschen lesbaren *Assembly-Code* umgewandelt wird. Zum anderen Dekompilieren, hier gelingt die *Rückumwandlung von Bytecode* in die *ursprüngliche Programmiersprache*.

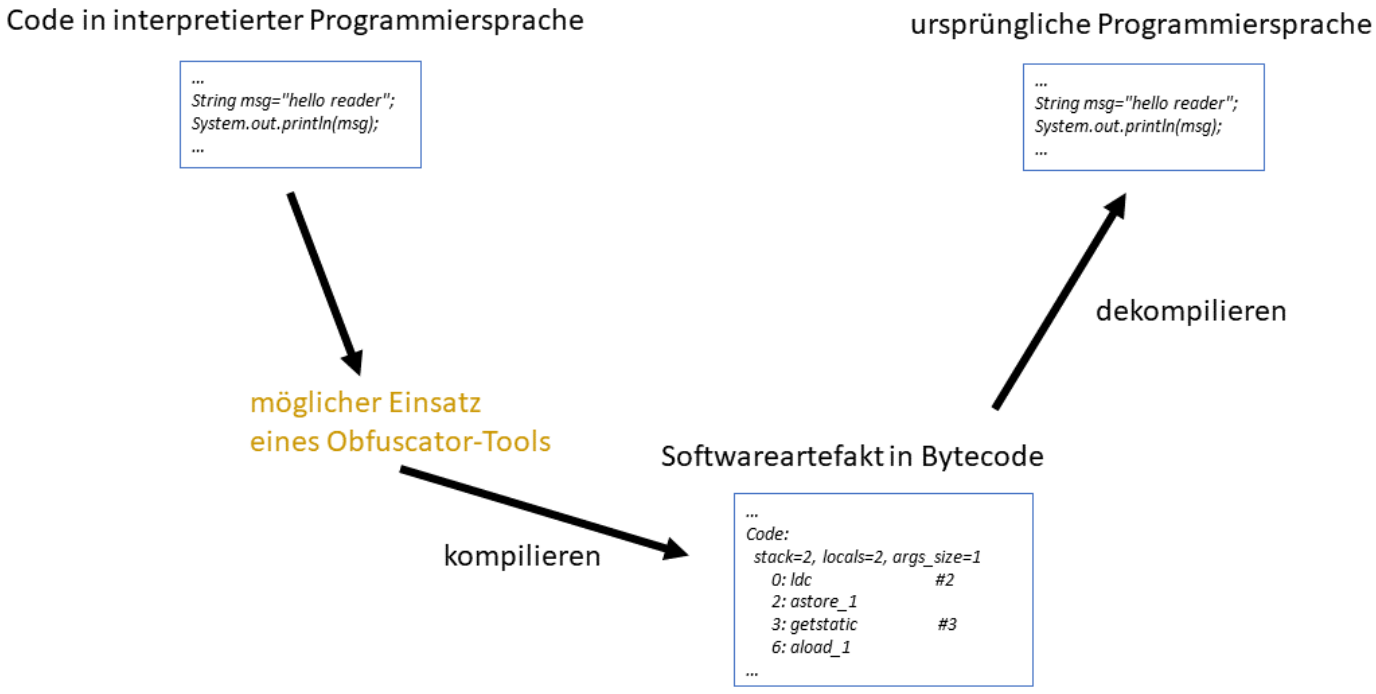


Disassemblieren

Disassemblieren wird bei Softwareartefakten eingesetzt, welche in Form von binärer oder hexadezimalen Maschinensprache vorliegen. Diese entsteht durch die Kompilierung von Hochsprachen wie C oder C++. Beim Kompilierungsprozess werden viele Optimierungsmassnahmen vom eingesetzten Compiler für die Zielplattform durchgeführt. Das daraus resultierende Programm wird dadurch schneller, jedoch gehen Metainformationen vom ursprünglichen Programmiercode, wie zum Beispiel Bezeichnungen von Variablen und Funktionen, verloren. Deshalb ist eine Rückumwandlung in die ursprüngliche Programmiersprache nicht möglich, stattdessen kann *Maschinencode in Assembly* umgewandelt werden. Somit können die einzelnen Operationen und Speicherzugriffe nachvollzogen werden. Für das Disassemblieren werden professionelle Tools eingesetzt, welche den *Pfad der Ausführung* nachvollziehen und Sprünge innerhalb des Codes in verständlicher Form darstellen können.

Dekompilieren

Bei interpretierten Programmiersprachen wie Java oder C# wird der Programmcode nicht in Maschinencode, sondern in Bytecode kompiliert. Der Bytecode wiederum wird zur Laufzeit von einer virtuellen Maschine, zum Beispiel der Java Virtual Machine, interpretiert und auf dem Zielsystem ausgeführt. Der Bytecode ist teilweise bereits optimiert, enthält aber noch Metainformationen, was die Rückumwandlung in die ursprüngliche Programmiersprache ermöglicht. Je nachdem wie die Kompilierung erfolgte,



kann der Bytecode vollständig zurückübersetzt werden.

TECHNIKEN, UM REVERSE ENGINEERING ZU ERSCHWEREN

Das Ergebnis von Disassemblieren oder Dekompilieren wird hauptsächlich durch die *Konfiguration des Compilers* sowie weiteren Tools, wie der *Einsatz eines Obfuscator-Tools*, beeinflusst. Obfuscator-Tools setzen unterschiedlichste Techniken ein, um Reverse Engineering zu erschweren. Es gibt sie für sämtliche Programmiersprachen und viele sind als Open Source zum Beispiel auf Github zu finden. Ein Obfuscator-Tool wird vor dem Kompilieren auf den Programmiercode angewendet. Sie setzten unter anderem auf das Umbenennen von Variablen- und Methodennamen zu zufällig generierten Zeichenabfolgen, bauen zusätzliche Iterationen, Verschachtelungen und Abfragen mit ein. Teilweise werden eingesetzte Variableninhalte verschlüsselt abgelegt und gängige Programmierentwurfsmuster in komplexe unverständliche Abfolgen umgebaut, um Decompilers zu verwirren und so ein inkorrektes Ergebnis zu erzeugen. Code und Metainformationen, welche nicht zum Kompilieren benötigt werden, werden entfernt, um zukünftigen Angreifern so wenig Informationen wie möglich zu überlassen. Die Aufzählung der Techniken ist bei weitem nicht vollständig, oft werden auch eigene Kreationen oder Variationen zur Verschleierung des Quellcodes eingesetzt.

Ein Obfuscator-Tool wird eingesetzt, wenn Entwickler den *Zugang zum Quellcode* des eigenen Produkts, ihr geistiges Eigentum, *verunmöglichen oder erschweren* wollen. Bei der Entwicklung von Malware werden oft Obfuscator-Tools verwendet, verschiedene Zeichencodierungen und auch Verschlüsselung auf den Quellcode angewendet, um den *Fähigkeitslevel der Malware Analysten* und den *Zeitaufwand der Analyse* zu erhöhen. Zudem kommen oftmals noch Anti-Debugging Techniken zum Einsatz, welche in diesem Artikel jedoch nicht weiter beleuchtet werden.

Durch den Einsatz oben beschriebener Verschleierungstechniken, verhindern die Entwickler von Schadsoftware ebenfalls die Erkennung ihrer Malware durch automatische Analysen von Anti-Virenlösungen.

VORSTELLUNG AKTUELLER RESERVE ENGINEERING TOOLS

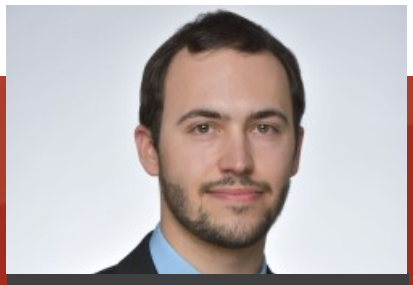
- **Ghidra** ist ein Open Source Reverse Engineering Framework programmiert und supported von der Forschungsabteilung der National Security Agency (NSA). Ghidra ist ein sehr mächtiges und breit aufgestelltes Framework, welches eine Vielzahl an nützlichen Tools auf den gängigen Plattformen Windows, macOS und Linux mitbringt.

- **dotPeek** ist ein kostenloser .Net Decompiler und Assembly Browser von JetBrains. Damit lassen sich .NET Assemblys einfach in C# oder Intermediate Language (IL) rückübersetzten.

- **IDA Pro** ist ein sehr funktionsumfangreicher Disassembler und Debugger von Hex Rays. IDA Pro ist weitverbreitet in der Malware Analyse und der Vulnerability Forschung. Hex Rays bietet mit dem IDA Free ebenfalls eine abgespeckte gratis Version von IDA Pro an.

FAZIT

Reverse Engineering ist eine der wichtigsten Techniken in der Analyse von Malware und allgemein eine sehr hilfreiche Tätigkeit beim Entdecken von Schwachstellen in unterschiedlichen Produkten. Zudem ist Reverse Engineering auch in anderen unterschiedlichen Bereichen wertvoll und sollte daher nicht in Vergessenheit geraten. Disassemblieren und Dekompilieren können hilfreich sein bei Blackbox Tests von Software, um weiterführende Informationen und mögliche Angriffspunkte identifizieren zu können. Obfuscator-Tools erschweren das Reverse Engineering und es gibt sie beinahe wie Sand am Meer.



Ralph Meier

next gen vulnerability intelligence

VulDB

Vulnerability Management mit Splunk

Laden Sie einfach und unkompliziert die Daten für das Vulnerability Management Ihrer Umgebung in Splunk. Die frei installierbare Applikation nutzt die offene API von VulDB, um Daten einzulesen, abzulegen und aufzuarbeiten. Noch nie war Vulnerability Management so einfach. Setzen Sie sich mit uns in Verbindung!

)SCIP(
official data provider

> https://vuldb.com

MICHÈLE TREBO

SIEGELUNG IM STRAFPROZESS

In Nachschlagewerken wird die *Siegelung* oft als Prozess definiert, bei dem eine Sache mit einem Siegel versehen wird, hat allerdings, wie der nachfolgende Abschnitt zeigt, im Sinne der Strafprozessordnung eine sinnbildliche Bedeutung. Vermuten die Strafbehörden eine zu ergreifende Person und/oder Beweismittel, ordnet die Staatsanwaltschaft schriftlich eine Durchsuchung an. Diesem Durchsuchungsbefehl gehen meist, wie im Flussdiagramm dargestellt, entweder eine polizeiliche Anhaltung oder polizeiliche Ermittlungen, unter anderem aufgrund einer Anzeige voran.

Die Siegelung als *Sofortmassnahme* garantiert, dass die Strafbehörden sichergestellte Gegenstände und/oder Aufzeichnungen weder einsehen noch verwenden. Wie es genau zur Siegelung kommt und wie sie aufgehoben werden kann, wird in den nachfolgenden Abschnitten erörtert.

POLIZEILICHE ANHALTUNG

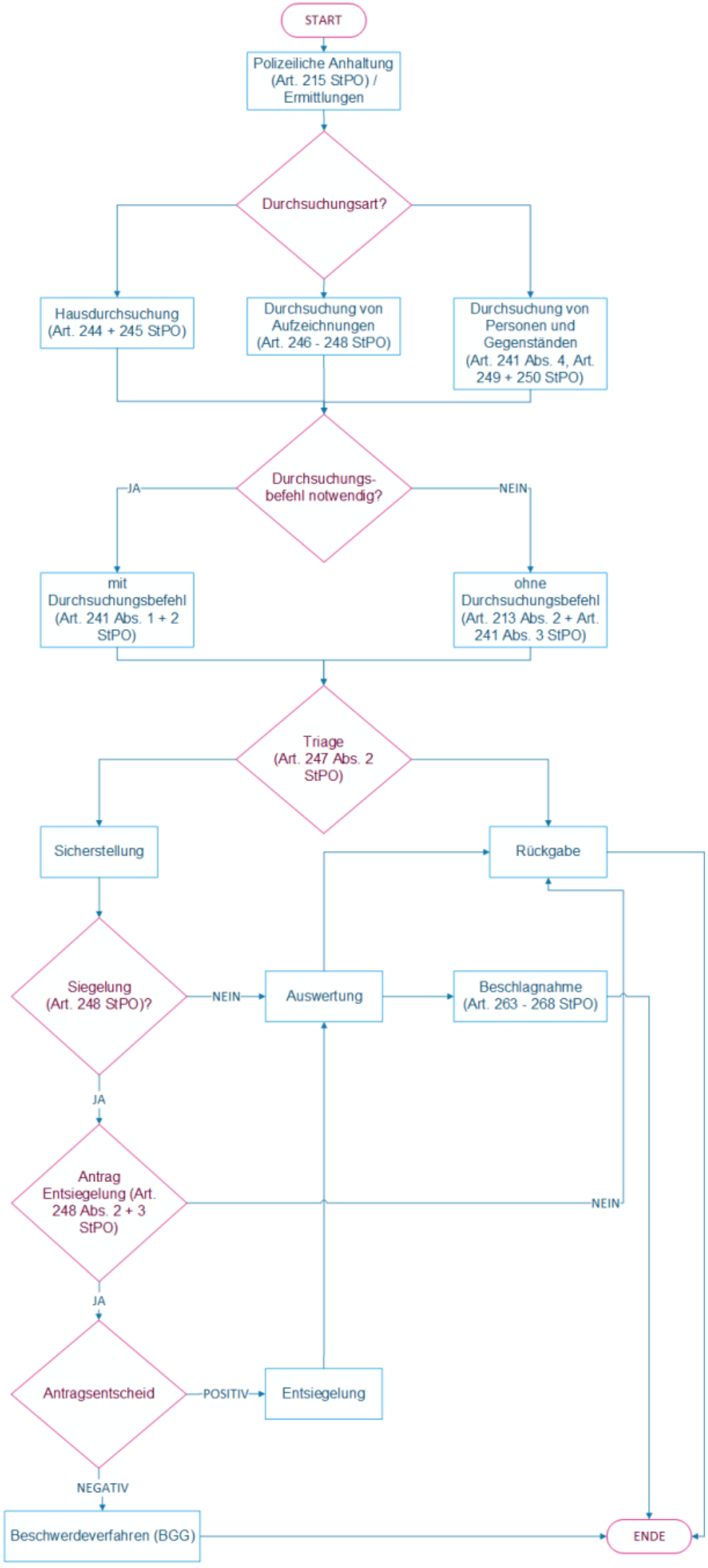
Die Polizei ist im Rahmen der polizeilichen Anhaltung berechtigt, ohne Anordnung bzw. ohne Durchsuchungsbefehl der Staatsanwaltschaft, eine Person anzuhalten, ihre Identität festzustellen, sie kurz zu befragen, abzuklären, ob sie eine Straftat begangen hat und ob nach ihr oder nach Gegenständen, die sich in ihrem Gewahrsam befinden, gefahndet wird und darf sie wenn nötig auf die Polizeistation mitnehmen. Die angehaltene Person ist verpflichtet, ihre Personalien anzugeben, Ausweispapiere vorzulegen, mitgeführte Sachen vorzuzeigen sowie Behältnisse oder Fahrzeuge zu öffnen.

DURCHSUCHUNG

Die Strafprozessordnung sieht unterschiedliche Arten von Durchsuchungen vor. Dabei unterscheidet sie zwischen *Hausdurchsuchungen*, *Durchsuchungen von Aufzeichnungen* und *Durchsuchungen von Personen und Gegenständen*. Damit die Polizei Durchsuchungen durchführen darf, braucht sie grundsätzlich einen *schriftlichen Durchsuchungsbefehl* der Staatsanwaltschaft. Wie in den nachfolgenden Praxisbeispielen beschrieben, gibt es allerdings *Ausnahmen*.

Durchsuchung mit Durchsuchungsbefehl

Ein Elektronikgeschäft stellt fest, dass seit Kurzem vermehrt Verkaufsmaterial verschwindet und schaltet die Polizei ein. Auf einer der Überwachungsauf-


START
Polizeiliche Anhaltung (Art. 215 StPO) / Ermittlungen
Durchsuchungsart?
Hausdurchsuchung (Art. 244 + 245 StPO)
Durchsuchung von Aufzeichnungen (Art. 246 - 248 StPO)
Durchsuchung von Personen und Gegenständen (Art. 241 Abs. 4, Art. 249 + 250 StPO)
Durchsuchungs-befehl notwendig?
JA
NEIN
mit Durchsuchungsbefehl (Art. 241 Abs. 1 + 2 StPO)
ohne Durchsuchungsbefehl (Art. 213 Abs. 2 + Art. 241 Abs. 3 StPO)
Triage (Art. 247 Abs. 2 StPO)
Sicherstellung
Rückgabe
Siegelung (Art. 248 StPO)?
NEIN
Auswertung
Beschlagnahme (Art. 263 - 268 StPO)
JA
Antrag Entsiegelung (Art. 248 Abs. 2 + 3 StPO)
NEIN
JA
Antragsentscheid
POSITIV
Entsiegelung
NEGATIV
Beschwerdeverfahren (BGG)
ENDE

nahmen ist zu sehen, wie eine angestellte Person eine Spiegelreflexkamera aus dem Regal nimmt und damit zur Umkleide der Mitarbeiter geht. Kurz darauf ist erkennbar, dass die Person ohne die Spiegelreflexkamera die Umkleide wieder verlässt. Nach Prüfung des Schichtplans stellt die Polizei fest, dass die Schichten dieser angestellten Person mit dem Verschwinden des Verkaufsmaterials übereinstimmen. Daraufhin nimmt die Polizei mit der zuständigen Staatsanwaltschaft Kontakt auf und bittet um einen Durchsuchungsbefehl. Sie vermutet am Wohnort, auf elektronischen Geräten und im Garderobenschrank der beschuldigten Person Beweismittel. Da nur die Geschäftsleitung des Elektronikgeschäfts und die Polizei über die Ermittlungen Bescheid wissen, somit also *keine Gefahr im Verzug* vorliegt, wartet die Polizei den *schriftlichen Durchsuchungsbefehl* der Staatsanwaltschaft ab und plant anschliessend die Durchsuchungen.

Findet die Polizei beim Anhalten einer Person in dessen Tasche mehrere kleine Mini-Grip-Säckchen mit weissem Pulverinhalt, eine hohe Summe Bargeld und mehrere Mobiltelefone, so stellt sie die Sachen aufgrund des Verdachts auf Verstoss gegen das *Betäubungsmittelgesetz* sicher und nimmt die beschuldigte Person mit auf die Polizeistation. Da die Polizei weitere Beweismittel in der Wohnung der beschuldigten Person vermutet, bittet sie die Staatsanwaltschaft um einen Durchsuchungsbefehl. Da die Gefahr besteht, dass eine mögliche Mittäterschaft bereits von der Verhaftung der beschuldigten Person erfahren hat und so *Beweismittel gefährdet* sind, erteilt die Staatsanwaltschaft der Polizei einen *mündlichen Durchsuchungsbefehl* und reicht diesen in schriftlicher Form nach. Damit kann die Polizei unmittelbar nach der Verhaftung der beschuldigten Person dessen Räume durchsuchen ohne, dass sie den schriftlichen Durchsuchungsbefehl der Staatsanwaltschaft abwarten muss.

Durchsuchung ohne Durchsuchungsbefehl

Eine Frau wählt um zwei Uhr morgens den Notruf der Polizei und meldet, dass ihre vierjährige Tochter nicht mehr in ihrem Bett liege. Sie mache sich grosse Sorgen, da ihr gewalttätiger Mann und sie am Abend zuvor eine heftige Auseinandersetzung bezüglich des Sorgerechts der Tochter hatten und er gedroht habe, ihr die Tochter wegzunehmen. Er habe gesagt, dass er sich mit ihr ins Ausland abzusetzen wolle. Ihr Mann und sie seien getrennt und er lebe unterdessen

in einer Wohnung etwa eine Stunde von ihr entfernt. Er habe aber noch den Schlüssel ihrer Wohnung. Während eine Polizeipatrouille sich auf den Weg zum Wohnort der Mutter macht, fährt die zweite Patrouille an den neuen Wohnort des Vaters des Kindes. Bei dessen Wohnung angekommen, öffnet niemand die Tür. Plötzlich hört die Polizeipatrouille ein weinendes Kind. Da dieses Weinen aus der Wohnung des Verdächtigen zu kommen scheint und er für seine Gewaltbereitschaft bereits bekannt ist, entscheiden sich die Polizeifunktionäre, die Wohnungstüre einzutreten. Da in diesem Fall das vierjährige Kind in Gefahr sein könnte, somit also *Gefahr im Verzug* vorliegt, darf die Polizeipatrouille *ohne Durchsuchungsbefehl* die Wohnung betreten. Sie informiert die Staatsanwaltschaft unverzüglich, nachdem sie die Lage unter Kontrolle gebracht hat.

TRIAGE

Findet die Polizei bei einer Durchsuchung Gegenstände und/oder Aufzeichnungen, die als *Beweismittel* in einem Strafverfahren von Bedeutung sein könnten, stellt sie diese sicher. Es reicht für eine Sicherstellung aus, wenn unter anderem auf einem Datenträger, der vor Ort nicht gesichtet werden kann, Beweismittel vermutet werden. Gegenstände und/oder Aufzeichnungen, die klar als Beweismittel ausgeschlossen werden können, werden der Person belassen.

Siegelung

Möchte eine Person nicht, dass ihre sichergestellten Gegenstände und/oder Aufzeichnungen beschlagnahmt und gesichtet werden, so kann sie die *Siegelung* verlangen. In diesem Fall nimmt die Polizei zwar die *Sicherstellungen* mit, darf sie aber *nicht auswerten*. Die Staatsanwaltschaft hat *20 Tage* Zeit zu entscheiden, ob sie beim Zwangsmassnahmengericht ein Gesuch auf Entsiegelung stellen will. Da die Sicherstellungen der Polizei aber meist für das Strafverfahren relevante Spuren enthalten, entscheidet sich die Staatsanwaltschaft in den häufigsten Fällen für den Entsiegelungsantrag. Sollte es aber trotzdem vorkommen, dass die Staatsanwaltschaft keinen Antrag auf Entsiegelung stellt, so werden die Sicherstellungen der Person zurückgegeben. Stellt die Person keinen Antrag auf Siegelung, so werden die Sicherstellungen ausgewertet. Je nachdem, ob sich herausstellt, dass die Sicherstellungen für den Strafprozess

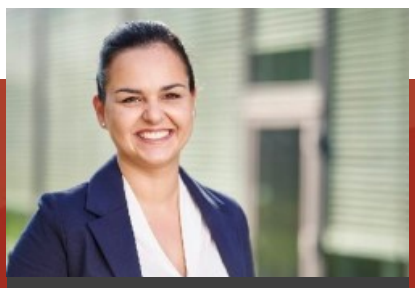
relevant sind oder nicht, werden sie beschlagnahmt oder zurückgegeben.

Antragsentscheid

Entscheidet sich das *Zwangsmassnahmengericht* für die Entsiegelung, so werden die Sicherstellungen ausgewertet und entweder beschlagnahmt oder der Person zurückgegeben. Lehnt das Zwangsmassnahmengericht den Entsiegelungsantrag der Staatsanwaltschaft ab, so kann ein *Beschwerdeverfahren* eingeleitet werden.

ZUSAMMENFASSUNG

Vermutet die Strafbehörde eine zu ergreifende Person und/oder Beweismittel, hat sie das Recht, Durchsuchungen durchzuführen und Beweismittel sicherzustellen. Die Person, die das Eigentum an den sichergestellten Sachen besitzt, kann die Siegelung verlangen, möchte sie verhindern, dass die Strafbehörden die Gegenstände und/oder Aufzeichnungen auswerten. Die Siegelung kann auf Antrag der Staatsanwaltschaft durch das Zwangsmassnahmengericht aufgehoben und die Beweismittel zur Auswertung freigegeben werden.



Michèle Trebo

WEITSICHT HILFT BEIM VERHINDERN UND EINDÄMMEN VON RISIKEN

Bildquelle: https://pixabay.com/images/id-6911736/

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