MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE JUNI 2023
RANSOMWARE UND COMPLIANCE

SO SCHULDIG SIND OPFER VON RANSOMWARE

Es ist unbestritten, dass Ransomware als das Hauptrisiko der heutigen Zeit gilt. Doch wie schuldig sind die Opfer von Ransomware tatsächlich?

AUDITD KONFIGURIEREN FÜR COMPLIANCE

Wir zeigen auf, wie ein einfaches Wort innerhalb eines Steuerelements zu einer komplizierten Konfigurationsdatei werden kann, welche erhebliche Auswirkungen auf das System hat, wenn man von einem hochrangigen Sicherheitsrahmen ausgeht.

June 2023: Zeitalter des Schmerzes

Die letzten Tage waren geprägt von *Ransomware–Angriffen* und *DDoS-Attacken* auf kritische Anbieter in der Schweiz. Eine *Russische Gruppierung* hat sich zu diesen bekannt und wollte damit aufzeigen, dass sie die Schweizer Unterstützung für die Ukraine nicht goutiert.

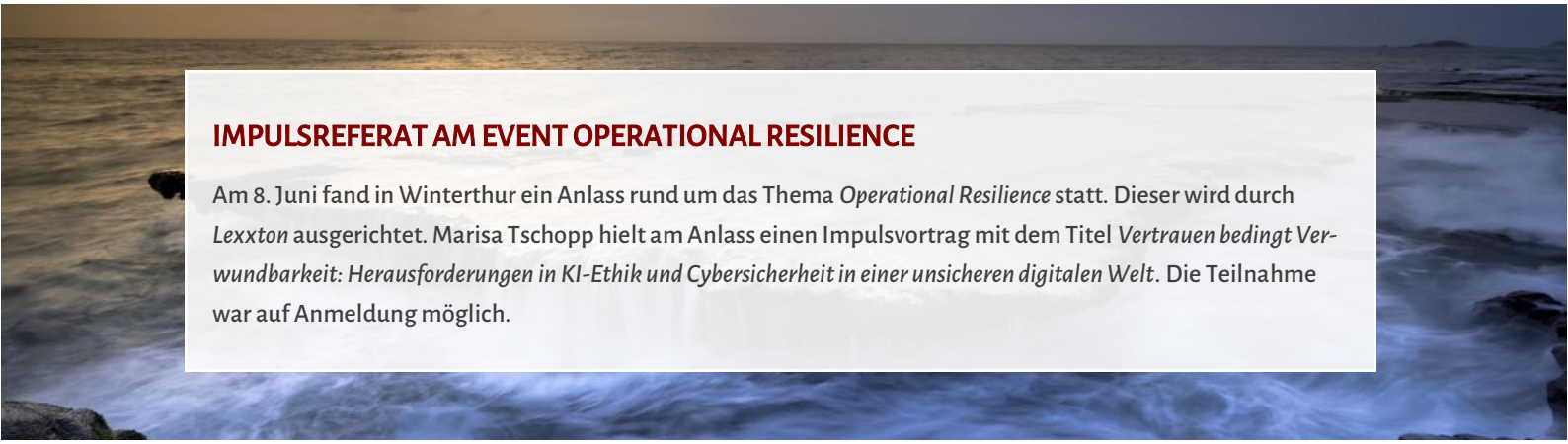
Dass diese Angriffe dermassen erfolgreichen waren zeigt, dass Schweizer Organisation halt noch immer nicht begriffen haben, welchen Stellenwert das Thema Cybersecurity in der heutigen Zeit einzunehmen hat. Die jahrelange Vernachlässigung des Themas ist dafür verantwortlich, dass das neue Zeitalter des Schmerzes überhaupt eingeführt werden kann.

Es wäre langsam an der Zeit, dass die Unternehmensführungen merken, dass sie nicht ewig den Kopf in den Sand stecken können. Ein Umdenken, ein Fokussieren ist gefragt. Doch solange das Management in Quartalszahlen denkt, wird sich das nicht ändern. Da helfen auch die plakativen Angriffe, die vermeintlich aus Russland stammen, nicht. Das Zeitalter des Schmerzes hat erst angefangen und wird noch ein paar Jahre anhalten.

Marc Ruef
Head of Research

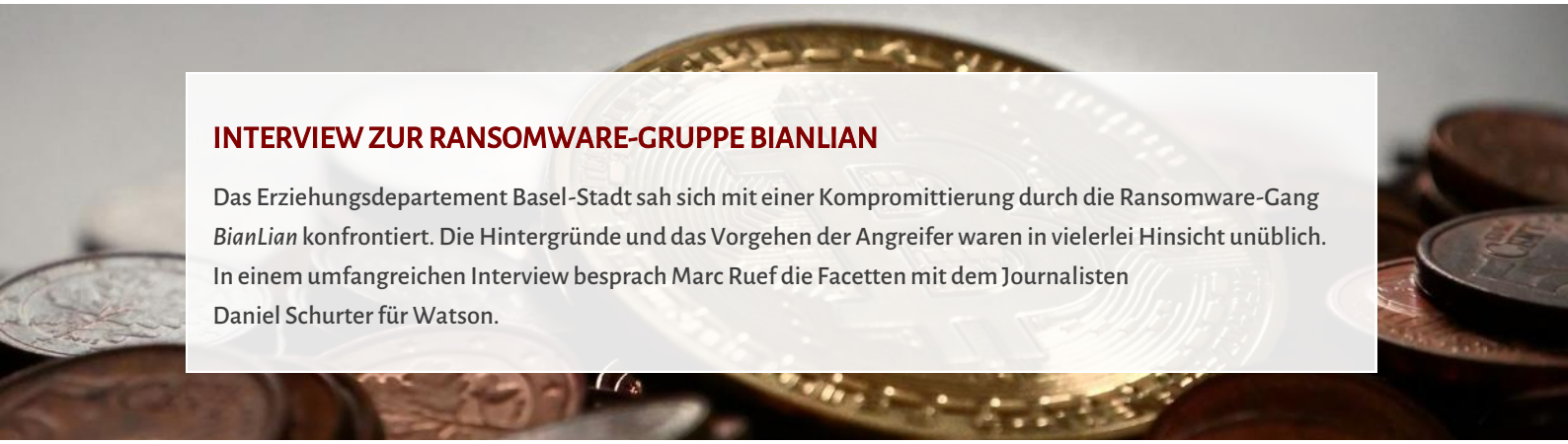
NEWS

WAS IST BEI UNS PASSIERT?



IMPULSREFERAT AM EVENT OPERATIONAL RESILIENCE

Am 8. Juni fand in Winterthur ein Anlass rund um das Thema *Operational Resilience* statt. Dieser wird durch *Lexxton* ausgerichtet. Marisa Tschopp hielt am Anlass einen Impulsvortrag mit dem Titel *Vertrauen bedingt Verwundbarkeit: Herausforderungen in KI-Ethik und Cybersicherheit in einer unsicheren digitalen Welt*. Die Teilnahme war auf Anmeldung möglich.



INTERVIEW ZUR RANSOMWARE-GRUPPE BIANLIAN

Das Erziehungsdepartement Basel-Stadt sah sich mit einer Kompromittierung durch die Ransomware-Gang *BianLian* konfrontiert. Die Hintergründe und das Vorgehen der Angreifer waren in vielerlei Hinsicht unüblich. In einem umfangreichen Interview besprach Marc Ruef die Facetten mit dem Journalisten Daniel Schurter für Watson.

VORTRAG AN ETH CYBER GROUP ALUMNI ZÜRICH EVENT

Am 11. Mai 2023 fand die ETH Cyber Group Alumni Zürich Cyber Pathways statt. Die Veranstaltung hatte das ZIel, über 30 Berufe in der Cybersicherheitsbranche vorzustellen. Die Teilnehmerinnen und Teilnehmer hatten die Möglichkeit, wertvolle Einblicke in die Welt der IT-Sicherheit zu gewinnen und die verschiedenen Karrierewege zu erkunden. Während der Veranstaltung konnte Marius Elmiger seine Leidenschaft für diesen Bereich teilen und wertvolle Einblicke in die Welt der IT-Sicherheit geben.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

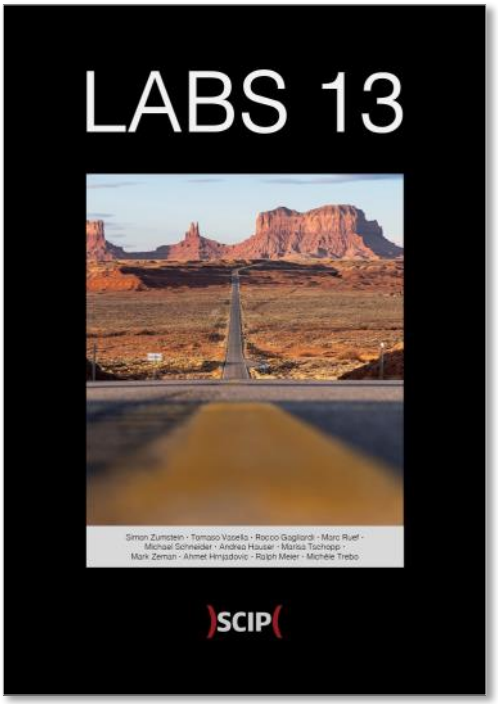
UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

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 auf unserer Webseite.



VORSICHT AUCH BEI SMISHING FALLEN

Bildquelle: https://unsplash.com/de/fotos/zs-41BroWhQ

MARC RUEF

SO SCHULDIG SIND DIE OPFER VON RANSOMWARE

Es ist unbestritten, dass Ransomware als das Hauptrisiko der heutigen Zeit gilt. Seit dem Erscheinen von WannaCry im Mai 2017 mehren sich die Zwischenfälle, die es in die Tagespresse schaffen. Die Opfer werden zu Zahlungen gezwungen oder sehen sich mit der Veröffentlichung von sensiblen Daten konfrontiert. Dieser Beitrag beleuchtet, ob und inwiefern die Opfer ihre Krisen mitverschuldet haben.

Bei Ransomware handelt es sich um eine spezielle Gattung klassischer Computerviren. Traditionell werden auf einem infizierten System die Daten verschlüsselt. Das Opfer wird kontaktiert und kann durch eine Lösegeldzahlung den Zugriff auf seine Daten zurückkaufen. Falls ein Backup der Daten vorhanden ist, kann das Opfer jedoch diesen Zwang umgehen. Die Ransomware-Gangs haben deshalb begonnen zuerst die Daten über das Netzwerk zu exfiltrieren, bevor sie durch eine lokale Verschlüsselung unzugänglich gemacht werden. Bei dieser Double-Exfiltration reicht das Zurückspielen eines Backups nicht mehr. Denn falls der Lösegeldzahlung nicht nachgekommen wird, werden die gestohlenen Daten veröffentlicht. Die Opfer sind, auch wenn sie alternative Lösungswege für den Zugriff auf ihre Daten erschlossen haben, gezwungen der Zahlung einzuwilligen.

DIE SCHULD

Unsere technokratische Gesellschaft verlangt eine digitale Transformation des Alltags. Unternehmen müssen dieser Pflicht der Digitalisierung folgen, um Akzeptanz zu erhalten und kompetitiv bleiben zu können. Dies führt zu elektronischen Informationsangeboten, Kommunikationskanälen und automatisierter Datenverarbeitung. Dadurch kann ein Mehr an Flexibilität und Effizienz gewährleistet werden. Vor allem Letztere wird durch die Unternehmen freien Willens angestrebt, um eine wirtschaftliche Optimierung erreichen zu können.

Doch diese digitale Transformation darf nicht geschehen, ohne das Thema Cybersecurity mitzuberücksichtigen. Es ist zwar möglich, eine vollumfängliche Digitalisierung ohne diese umzusetzen. Doch dadurch erhöht man seine Risiken. Jeder Mensch, jedes Unternehmen darf Risiken eingehen. Man muss sich aber bewusst sein, dass Risiken auch getragen werden können müssen. Wer sich entschie-

den hat Risiken zu tragen, darf sich nicht beklagen, wenn der schlechtesmögliche Zustand eintrifft. Die wenigsten von uns setzen sich ohne Sicherheitsgurt vors Lenkrad, fahren 100 kmh in einem Dorf oder überqueren eine dichtbefahrene Kreuzung ohne Kontrollblick. Wer es trotzdem tut, nimmt Schäden an Fahrzeugen, Personen und Umwelt in Kauf. Dabei spielt es eine untergeordnete Rolle, ob man diese Konsequenzen absichtlich oder fahrlässig akzeptiert genommen hat.

Der Autofahrer muss die anderen Verkehrsteilnehmer berücksichtigen. Bei der digitalen Transformation sind dies Mitarbeiter, Partner und Kunden. Wer also Digitalisierung ohne Cybersecurity macht, dem ist es weitestgehend egal, ob auch diese einen Schaden davontragen werden. Dies ist, man kann es nicht anders sagen, niederträchtig und verachtenswert.

Doch wieso erdreiste ich mich überhaupt anzunehmen, dass so manches Opfer das Thema Cybersecurity absichtlich oder fahrlässig nicht ernst genommen hat? Studiert man die einzelnen Fälle, wird es oftmals unverzüglich klar, dass dies der Fall gewesen sein muss. Betrachten wir die einzelnen Schritte, die für eine Kompromittierung mit einer Ransomware erforderlich sind:

Schritt Erfolgreiche Aktion Schutzmassnahme hat versagt

1. Mitarbeiter hat eine virenverseuchte Datei erhalten ⇨ Antiviren-Lösung auf Mail-Gateway, Antiviren-Lösung auf Client

2. Virenverseuchte Datei wurde ausgeführt ⇨ Mitarbeiter nicht gut geschult, Hardening des Mail-Client

3. Malware kann sich auf System etablieren ⇨ Hardening des Betriebssystems

4. Malware kann sich im Netzwerk propagieren ⇨ Netzwerksegmentierung, Firewalling, Dateirechte auf Netzwerkfreigaben, Log und Alerting

5. Ransomware kann Dateien exfiltrieren ⇨ Anomalien in der Traffic-Analyse, Data Loss Prevention

6. Ransomware kann Daten verschlüsseln ⇨ Lokale Dateirechte, Anomalien in der Zugriffs, Analyse, kein Backup

7. Ransomware kann ein Backdooring durchführen ⇨Patches/Updates, Hardening, Antiviren-Lösung auf Systemen

Diese Liste illustriert, dass ein erfolgreicher Ransomware-Angriff verschiedene Phasen durchlaufen muss und deshalb ein relativ hohes Mass an Komplexität mitbringt. In jeder dieser Phasen gibt es mehrere altbewährt Massnahmen, die sich mit überschaubarem Aufwand konsequent etablieren lassen. Wenn auch nur eine oder zwei dieser Massnahmen gegeben gewesen wären, hätte dies gereicht, um den erfolgreichen Ablauf zu unterbrechen und somit die Attacke abzuwenden. Dass ein Grossteil dieser Massnahmen fehlt oder nicht richtig umgesetzt ist, ist in erster Linie der Fahrlässigkeit des Opfers geschuldet. Art. 7 Abs. 1 DSG bringt es auf den Punkt:

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

DIE SÜHNE

Kein Unternehmen möchte mit negativen Schlagzeilen in den Medien sein. Da man nach einem Zwischenfall ungern in den sauren Apfel beissen möchte, zögern die meisten Betroffenen eine Veröffentlichung heraus. Das Vogel-Strauss-Prinzip wird also konsequent weitergeführt, in dieser Phase jedoch aus anderen Beweggründen. Man hofft, dass sich das Problem von alleine lösen wird.

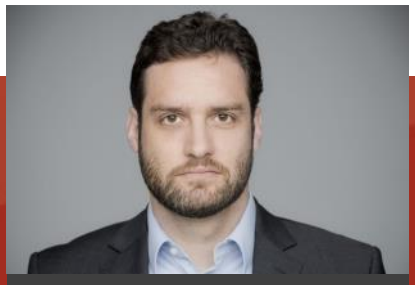
Die Konsequenz dieses Zögerns ist oftmals, dass die betroffenen Personen – Mitarbeiter, Partner und Kunden – nicht oder erst spät über vom Zwischenfall erfahren. Dabei hätte das Unternehmen die moralische Pflicht – und manchmal auch eine rechtliche Vorgabe (z.B. Art. 34 Abs. 1 DSGVO) -, sie über die drohenden Risiken zu informieren. Denn sie könnten nun Opfer von zielgerichtetem Phishing, Social Engineering, Datendiebstahl oder Erpressung werden. Doch Nein, die Unternehmen setzen ihren unprofessionellen Egoismus fort, überlassen die wahren Opfer ihrem unverschuldeten Schicksal.

Die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) sieht vor, dass in gewissen Fällen drakonische Strafen für einen fahrlässigen oder fehlerhaften Umgang mit Daten ausgesprochen werden kann (Art. 58 Abs. 2 sowie Art. 83 DSGVO). Die Überarbeitung des Datenschutzgesetz der Schweiz (DSG) will ebenfalls solche Einführen. Doch juristischer Ermessensspielraum führen nicht selten dazu, dass die Gesetze wie zahnlose Papiertiger wirken. Sie vermögen nachträglich nicht den Schmerz auszulösen, um vorgängig Dummheiten und Frechheiten zu verhindern.

So verbleiben zum Schluss nur noch die Betroffenen, in erster Linie die Kunden, die die gerechte Sühne durchsetzen können. Durch konsequentes Meiden von Anbietern, die sich nicht um die Datensicherheit kümmern, könnte ein Zeichen gesetzt werden. Und mit dem Umsetzen von Anzeigen liesse sich auch auf rechtlicher Ebene ein Signal geben. Doch Kunden sind träge und vergessen zu schnell. Was interessiert sie der Breach von vor einem halben Jahr? Und wohin will man wechseln? Zu einem anderen Anbieter, der das Thema nicht ernst nehmen wird? Ein Teufelskreis, bei dem es nur Verlierer gibt. Nur die Juristen vermögen diesen zu durchbrechen. Unternehmen und Entscheider müssen konsequent zur Rechenschaft gezogen werden. Und zwar nicht erst morgen, sondern schon heute.

FAZIT

Ransomware-Zwischenfälle haben sich die letzten Jahre gehäuft. Betrachtet man die Fälle im Detail, so wird klar, dass ihnen ein fehlendes oder fehlerhaftes Verständnis für das Thema Cybersicherheit zugrundeliegt. Risiken werden durch Unternehmen fahrlässig oder bewusst in Kauf genommen, die durch einzelne Massnahmen frühzeitig und nachhaltig hätten mitigiert werden können. Nicht selten werden Drittparteien betroffen, die keinen direkten Einfluss auf das Sicherheitsniveau einer Unternehmung ausüben können und dadurch zu wehrlosen Opfern werden. Hierbei sollte die Gesetzgebung konsequent ansetzen und nachlässige Firmen in die Pflicht nehmen.


Marc Ruef

Sie brauchen Unterstützung?

In der mobilen Arbeitswelt ist eine umfangreiche Cyber-Strategie unumgänglich. Unternehmen in der Schweiz sind mittlerweile täglich von DDoS Attacken, Internetkriminalität und gezielten Phishingversuchen betroffen. Die scip AG unterstützt durch ihre Expertise im Bereich Cybersecurity und das frühzeitige Erkennen von IT Schwachstellen, um Internetkriminellen keine Chance zu geben.

SCIP

> https://www.scip.ch

ROCCO GAGLIARDI

AUDITD KONFIGURIEREN FÜR COMPLIANCE

Während unserer Bewertungen müssen wir bestätigen, dass ein System Audit-Protokolle korrekt erzeugt und verarbeitet. Da es keine spezifischen Anforderungen gibt, liegen die Anzahl und die Art der erzeugten Aufzeichnungen in erster Linie in unserem Ermessen, basierend auf dem verwendeten Kontrollrahmen.

Die Erfahrung des Auditors bestimmt, ob die generierten Protokollkategorien auf der Grundlage der analysierten Situation ausreichend sind. Nehmen wir jedoch die Rolle eines Ingenieurs an, der mit der Konfiguration von auditd auf einem Linux-System beauftragt ist, welche Konfigurationen müssen letztendlich aktiviert werden?

In diesem Artikel werden wir mit einer sehr hohen Kontrolle beginnen, zwischenzeitliche Anforderungen entwickeln und diese dann in eine auditd Konfiguration umsetzen.

ÜBERSETZEN SIE KONTROLLEN IN ANFORDERUNGEN

Wir verwenden häufig die CIS CSC V8 als Kontrollrahmen. Kapitel 8, das der "Audit Log Management" gewidmet ist, enthält mehrere Kontrollen, die eine System-Audit-Konfiguration erfordern:

8.2 – Collect Audit Logs – Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

8.5 – Collect Detailed Audit Logs – Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Wir haben eine allgemeine Vorstellung davon, welche Informationen gesammelt werden müssen, aber die Anforderungen müssen weiter geklärt werden. Der CIS Controls Navigator ordnet Steuerelemente verschiedenen Frameworks zu. Schauen Sie sich also an, was andere Frameworks erfordern, indem Sie die 8.2-Zuordnung erweitern. Wir scrollen hinunter zu

den PCI v4.0-Gruppen und entdecken feiner abgestufte Steuerelemente, aus denen wir einfach diejenigen auswählen können, die auf unseren Anwendungsfall zutreffen.

Wir können nun unsere Zwischenanforderungen erstellen:

- Audit-Protokolle erfassen alle Aktionen, die von einer Person mit administrativem Zugriff durchgeführt werden, einschließlich der interaktiven Nutzung von Anwendungs- oder Systemkonten
- Audit-Protokolle erfassen alle ungültigen logischen Zugriffsversuche
- Audit-Protokolle erfassen alle Zugriffe auf Audit-Protokolle
- Audit-Protokolle erfassen alle Initialisierungen neuer Audit-Protokolle und alle Starts, Stopps oder Pausen der vorhandenen Audit-Protokolle
- Audit-Protokolle erfassen alle Änderungen an Identifikations- und Authentifizierungsdaten, einschließlich, aber nicht beschränkt auf: Erstellung neuer Konten; Erhöhung der Berechtigungen; alle Änderungen, Hinzufügungen oder Löschungen von Konten mit administrativem Zugriff
- Audit-Protokolle erfassen alle nicht autorisierten Zugriffsversuche auf Dateien
- Audit-Protokolle erfassen alle Änderungen der MAC-Richtlinien (SELinux)
- Audit-Protokolle erfassen die gesamte Nutzung von Medien (USB-Sticks, externe Festplatten usw.)
- Audit-Protokolle erfassen alle Zeitänderungen
- Audit-Protokolle erfassen alle Erstellungen und Löschungen von Objekten auf Systemebene

- Machen Sie die auditd-Konfiguration unveränderbar (um sie zu ändern, ist ein Neustart erforderlich)

Dieser Artikel bezieht sich auf CIS CSC V8, um die Beziehung zwischen High-Level-Kontrollen und Low-Level-Konfiguration zu veranschaulichen. Sie könnten die sehr detaillierten Sicherheitskontrollen, die z.B. in CIS Linux Server beschrieben sind, einfach implementieren, aber wir empfehlen, sie erst zu verwenden, nachdem Sie die Auswirkungen der Konfiguration auf das System verstanden haben.

AUDITD KONFIGURATION

Da wir nun die Anforderungen kennen, können wir mit der auditd-Konfiguration auf niedriger Ebene fortfahren. Die auditd-Regeln legen fest, welche Ereignisse geprüft werden sollen. Die Regeln werden in der Datei */etc/audit/rules.d/audit.rules* definiert.

Fügen Sie mit einem Editor Ihrer Wahl Regeln in der Datei hinzu oder ändern Sie sie entsprechend Ihren Anforderungen an die Überwachung. Die Syntax für die Regeln folgt der Syntax des Befehls *auditctl*. Um zum Beispiel Änderungen an der Datei */etc/passwd* zu überwachen, können Sie die folgende Regel hinzufügen:

```
## /etc/passwd monitor for write/change
-a always,exit -F path=/etc/passwd -F perm=wa
-F key=passwd-changes
```

Diese Regel filtert Schreib- (w) und Attribut- (a) Änderungen an der Datei */etc/passwd* und verknüpft sie mit dem Schlüssel *passwd_changes*. Um die Regeln zu konfigurieren, lesen Sie *auditctl(8) – Linux manual page (missing link!)*

BEGINNEN SIE MIT EINER SAUBEREN REGELBASIS

Es ist eine gute Praxis, mit einer leeren Regelbasis zu beginnen und einige Parameter einzustellen.

```
## Clean all rules
-D
## Increase buffer to survive stressful
situation
-b 8192
## Set failure mode to panic if the system
should stop in case of auditd error
## Enable this if the system must not work
```

```
without a functional audit log
# -f 2
```

Requirement: Audit Logs Capture All Actions Taken by Any Individual with Administrative Access, Including Any Interactive Use of Application or System Accounts

Dies erfordert die Konfiguration des Tools *pam_tty_audit*. Ausgehend von Unix PAM bietet Linux PAM (Pluggable Authentication Modules) flexible Authentifizierungsdienste für Anwendungen und Systemdienste. Die Komponenten Konto, Authentifizierung, Passwort und Sitzung regeln die Authentifizierungsfunktionen.

Mit der Option *enable in /etc/pam.d/system-auth* und */etc/pam.d/password-auth* können Sie die TTY-Eingabe eines Benutzers überprüfen. Die Konfigurationsparameter finden Sie unter *pam_tty_audit(8) – Linux manual page*.

Dies gilt auch für "Audit-Protokolle erfassen alle ungültigen logischen Zugriffsversuche", da sowohl gültige als auch ungültige Aktionen überprüft werden.

Requirement: Audit Logs Capture All Access to Audit Logs

Die Überwachung der auditd-Komponenten bietet Einblick in den Audit-Prozess, gewährleistet die Integrität der Audit-Protokolle, validiert die Konfiguration und erhält den Systemzustand aufrecht.

Dies umfasst auch "Audit-Protokolle erfassen alle Initialisierungen neuer Audit-Protokolle und alle Starts, Stopps oder Pausen der bestehenden Audit-Protokolle".

```
## Access to all audit trails.
-a always,exit -F dir=/var/log/audit/ -F
perm=r -F auid>=1000 -F auid!=unset -F
key=access-to-audit-objects
-a always,exit -F path=/usr/sbin/aulast -F
perm=x -F key=access-to-audit-objects

-a always,exit -F path=/usr/sbin/aulastlogin
-F perm=x -F key=access-to-audit-objects
-a always,exit -F path=/usr/sbin/aureport -F
```

```
perm=x -F key=access-to-audit-objects
-a always,exit -F path=/usr/sbin/ausearch -F
perm=x -F key=access-to-audit-objects
-a always,exit -F path=/usr/sbin/auvirt -F
perm=x -F key=access-to-audit-objects
```

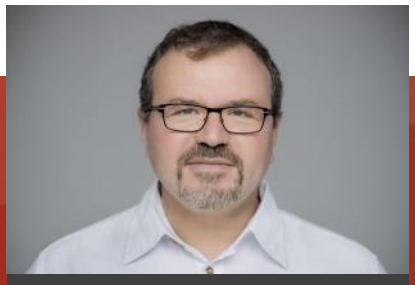
Requirement: Audit Logs Capture All Changes to Identification and Authentication Credentials

Audit-Protokolle müssen Änderungen an Identifizierungs- und Authentifizierungsdaten für die Untersuchung von Sicherheitsvorfällen, die Rechenschaftspflicht, die Einhaltung von Vorschriften, die Erkennung verdächtiger Aktivitäten, forensische Analysen und die Reaktion auf Vorfälle aufzeichnen.

```
## Elevation of privileges
-a always,exit -F arch=b64 -S setuid -F a0=0
-F exe=/usr/bin/su -F key=elevation-of-
privileges
-a always,exit -F arch=b32 -S setuid -F a0=0
-F exe=/usr/bin/su -F key=elevation-of-
privileges
-a always,exit -F arch=b64 -S setresuid -F
a0=0 -F exe=/usr/bin/sudo -F key=elevation-of
-privileges
-a always,exit -F arch=b32 -S setresuid -F
a0=0 -F exe=/usr/bin/sudo -F key=elevation-of
-privileges
-a always,exit -F arch=b64 -S execve -C uid!
=euid -F euid=0 -F key=elevation-of-
privileges
-a always,exit -F arch=b32 -S execve -C uid!
=euid -F euid=0 -F key=elevation-of-
privileges
## All changes, additions, or deletions to
accounts
-a always,exit -F path=/etc/group -F perm=wa
-F key=account-change
```

Wir haben gezeigt, wie ein einfaches Wort innerhalb eines Steuerelements zu einer komplizierten Konfigurationsdatei werden kann, die erhebliche Auswirkungen auf das System haben kann, wenn man von einem hochrangigen Sicherheitsrahmen ausgeht.

In Bezug auf das Framework ist es notwendig, Zwischenanforderungen zu entwickeln, die unabhängig voneinander in Low-Level-Konfigurationen umgewandelt werden können. Da sich jeder Filter auf die Leistung des Systems auswirkt, sollte jede Zwischenanforderung nur dann überprüft und konfiguriert werden, wenn sie notwendig ist oder wenn sie zu einer erhöhten Systemsicherheit beiträgt.



Rocco Gagliardi

MIT SCIP FRÜHZEITIG GEFAHREN ERKENNEN

Bildquelle: ttps://pixabay.com/users/noname_13-2364555/

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