# MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE APRIL 2024
VON CVSS 4.0 UND ACTIVE DIRECTORY

## WIESO CVSS 4.0 NICHT WIRKLICH BESSER WIRD

Unser Team hat das Common Vulnerability Scoring System genauer angeschaut und erklärt, wieso CVSS 4.0 wohl scheitern wird.

## IST ACTIVE DIRECTORY ANGREIFBAR?

Active Directory wird häufig zur Authentifizierung verwendet. Wie einfach solche Umgebungen anzugreifen sind, zeigen wir in unserem Artikel.

# April 2024: Unterwegs im Kosmos

Der Weltraum hat mich schon immer fasziniert. All diese Mysterien über seine Entstehung, seine endlosen Weiten, das Reisen durch den Raum. Wenn ich unser April Revue passieren lasse, dann waren auch wir in unserem Kosmos unterwegs, und konnten von unserer Reise, unseren Entdeckungen und Erforschungen berichten.

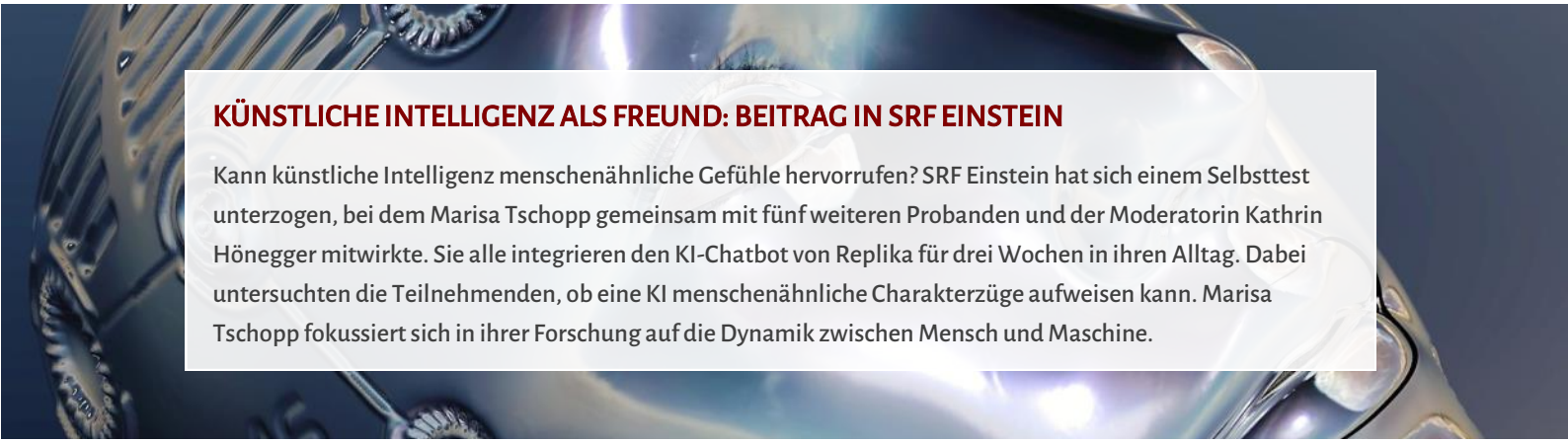
Der April ist auch bekannt für seine Launen und unvorhersehbaren Wetterumschwünge. Er erinnert uns daran, dass auch die Welt der Technologie ihre eigenen Stürme und Überraschungen mit sich bringt. Ich stelle mir zum Beispiel vor, wie ein Astronaut im All schwebt, und auf seine Ausrüstung und sein Training angewiesen ist, um sich den Herausforderungen des Weltraums zu stellen. So sind auch wir in unserem Business auf unsere Expertise, unser Verständnis für die Auswirkungen neuer Technologien und unser Feingefühl angewiesen.

Die Unberechenbarkeit und Vielschichtigkeit des Aprils können wir uns als gutes Vorbild nehmen, wenn wir neue Technologien einsetzen. Genau wie sich das Wetter im April schlagartig verändern kann, können auch unsere digitalen Ökosysteme zwischen Innovation und Unsicherheit schwanken. Daher wollen wir sicherstellen, dass unsere Reise in die digitale Welt von Menschlichkeit und Verantwortung begleitet wird. Lassen Sie uns gemeinsam neue Sterne und Planeten erkunden, aber nie vergessen, dass der wahre Kompass unserer Entdeckungen das menschliche Wohl und die Sicherheit aller sein sollte.

Serena Bolt
Research Team

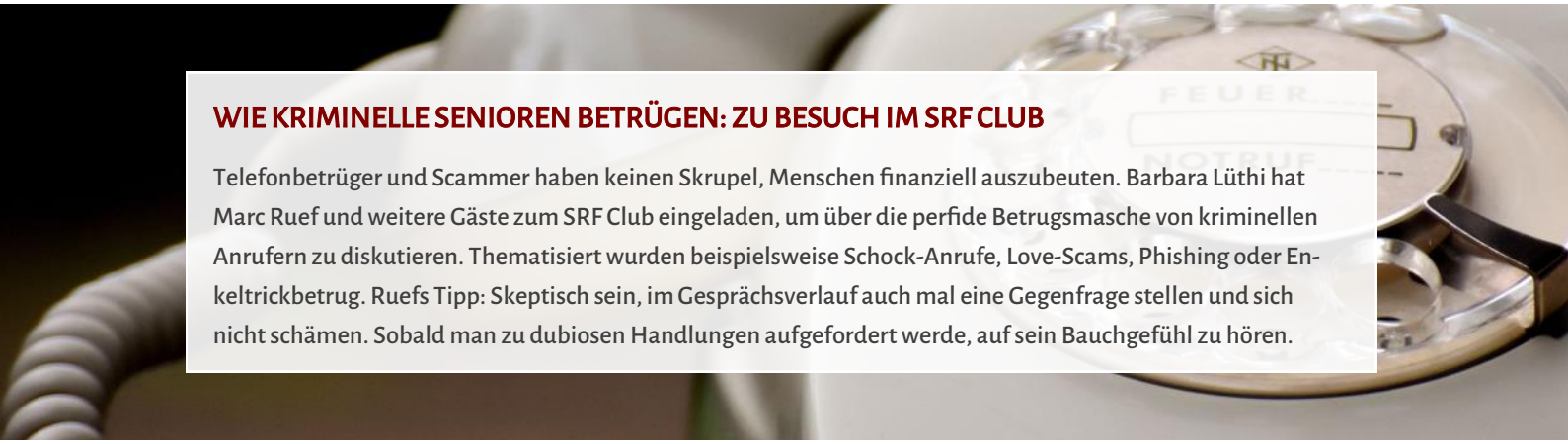
NEWS

# WAS IST BEI UNS PASSIERT?



## KÜNSTLICHE INTELLIGENZ ALS FREUND: BEITRAG IN SRF EINSTEIN

Kann künstliche Intelligenz menschenähnliche Gefühle hervorrufen? SRF Einstein hat sich einem Selbsttest unterzogen, bei dem Marisa Tschopp gemeinsam mit fünf weiteren Probanden und der Moderatorin Kathrin Hönegger mitwirkte. Sie alle integrieren den KI-Chatbot von Replika für drei Wochen in ihren Alltag. Dabei untersuchten die Teilnehmenden, ob eine KI menschenähnliche Charakterzüge aufweisen kann. Marisa Tschopp fokussiert sich in ihrer Forschung auf die Dynamik zwischen Mensch und Maschine.



## WIE KRIMINELLE SENIOREN BETRÜGEN: ZU BESUCH IM SRF CLUB

Telefonbetrüger und Scammer haben keinen Skrupel, Menschen finanziell auszubeuten. Barbara Lüthi hat Marc Ruef und weitere Gäste zum SRF Club eingeladen, um über die perfide Betrugsmasche von kriminellen Anrufern zu diskutieren. Thematisiert wurden beispielsweise Schock-Anrufe, Love-Scams, Phishing oder Enkeltrickbetrug. Ruefs Tipp: Skeptisch sein, im Gesprächsverlauf auch mal eine Gegenfrage stellen und sich nicht schämen. Sobald man zu dubiosen Handlungen aufgefordert werde, auf sein Bauchgefühl zu hören.

## POSTER-BEITRAG AN DER INTERACTIONS WITH LANGUAGE-BASED AI-KONFERENZ

Am 11. April 2024 konnte Marisa Tschopp einen Beitrag an der *Interactions with language-Based AI*-Konferenz halten. Unter dem Titel *Don't call me buddy!* teilte Marisa Erkenntnisse aus ihrer Forschung im Bereich Mensch-Maschine Interaktion am Leibniz-Institut für Wissensmedien (IWM). Das Netzwerk Mensch-Maschine-Interaktion des IWM hat in den letzten 4 Jahren das Zusammenspiel des Menschen mit Künstlicher Intelligenz bei der Verarbeitung natürlicher Sprache erforscht, und alle Ergebnisse an der Konferenz präsentiert.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

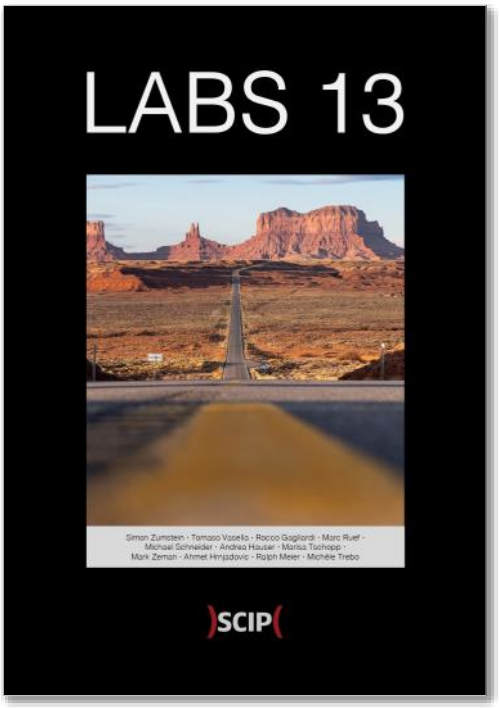
# UNSER AKTUELLES JAHRBUCH

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.



# WIESO CVSS 4.0 NICHT WIRKLICH BESSER WIRD

Bildquelle: https://unsplash.com/de/fotos/astronaut-im-raumanzug-schwebt-im-weltraum-Yj1M5riCKk4

MARC RUEF

# KONKRETE KRITIK AN CVSS 4.0
# WELCHE DINGE WERDEN NICHT BESSER

Das Common Vulnerability Scoring System (CVSS) konnte sich als Risikometrik im Bereich der technischen Cybersicherheit etablieren. Seit dem Erscheinen von CVSSv2 im Jahr 2007 wird der Ansatz breitflächig als Industriestandard verwendet, um Schwachstellen mit nachvollziehbaren Risiken zu versehen. Selbst die Verbesserungen in CVSSv3 haben das System aber nicht vor Kritik bewahrt. Der jüngst erschienene Nachfolger CVSSv4 stellt jedoch meines Erachtens einen konkreten Schritt in die falsche Richtung dar. Dieser Beitrag diskutiert, was schlechter wurde und warum ich hoffe, dass es sich nicht durchsetzen wird.

Unser Red Team ist bestens vertraut mit CVSS, denn schliesslich ist es fester Bestandteil unserer Risikoeinschätzungen, wie wir sie in Berichten und Präsentationen unseren Kunden zur Verfügung stellen. Hinzu kommt, dass scip knapp 20 Jahre für VulDB zuständig war und in dieser Zeit rund 150'00 Schwachstellen durch unser Moderationsteam mit CVSSv2 und CVSSv3 eingestuft wurde. Mittlerweile gehört VulDB nicht mehr zu scip. Dennoch begleiten wir auch dort gegenwärtige die Einführung von CVSSv4. Wir mussten uns also sowohl in Bezug auf Prozesse (z.B. Moderation) als auch technische Umsetzung (z.B. Implementierung, Kalkulationen, Parsing) sehr intensiv mit der neuen Iteration auseinandersetzen. Hierbei sind uns Eigenheiten aufgefallen, die sich als potentiell diskussionswürdige Paradigmenwechsel oder Unschönheiten abtun lassen. Sie erfordern ein Umdenken oder verhindern die Vergleichbarkeit mit den Scores der vorangegangenen Versionen. Manche Aspekte stellen jedoch eine konkrete Verschlimmbesserung dar, die so wohl nicht in Kauf genommen werden will. Diese könnten eine breite Akzeptanz der neuen Version verhindern.

## VIEL ZU LANGE VEKTOREN

Mit CVSS lassen sich quantitative Scores berechnen, die von 0.0 bis 10.0 reichen. Bevor ein solcher überhaupt berechnet werden kann, muss ein Vector String erstellt werden. Dieser besteht aus einzelnen Attributen, die die Beschaffenheit einer Schwachstelle skizzieren. Zum Beispiel wird der Attack Vector (AV) verwendet, um die Zugriffsmöglichkeiten eines Angriffs zu spezifizieren.

Ein `AV:N` bedeutet, dass der Angriff über das Netzwerk möglich ist. Andernfalls würde er AV:A für Adjacent Network (im LAN), AV:L für Local oder AV:P für Physical ausweisen.

Ein CVSSv2 Base Vector umfasst 6 Attribute. Eine nicht-authentisierte SQL-Injection, die sich über das Internet ausnutzen liesse, führt zu diesem simplen Vektor:

```
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
```

Eine der Verbesserungen von CVSSv3 war das Einführen zusätzlicher Attribute, wodurch die Beschaffenheit einer Schwachstelle mit einem Mehr an Granularität skizziert werden konnte. Plötzlich sind Attributsnamen nun entweder eine oder zwei Stellen lang. Neu Eingeführt wurden User Interaction (UI) und Scope (S). Beide haben im etablierten SQL-Injection-Scenario keinen Einfluss, wodurch sich der neue Vektor mit seinen 8 Attributen wie folgt gestaltet:

```
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
```

Mit CVSSv4 wurden weitere Attribute hinzugefügt. Zusätzlich zu Attack Complexity (AC) wird nun ebenfalls Attack Requirements (AT) genutzt und der seit CVSSv3 eher stiefmütterlich eingesetzte Scope (S) wurde gleich in drei Attribute der Subsequent System Impact Metrics aufgeteilt. Der neue Vektor für die gleiche SQL-Injection sieht dann mit seinen ganzen 11 Attributen so aus:

```
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/
VA:L/SC:N/SI:N/SA:N
```

Die Anzahl der minimal eingesetzten Attribute für den Base Score hat sich also seit CVSSv2 fast verdoppelt. Vorbei sind hiermit die Zeiten, in denen mit einem Blick die Struktur einer Schwachstelle ermittelt werden konnte. Die Simultanerfassung (Subitizing) des Menschen ist gar nicht mehr in der Lage, das zu tun, wird bei Erwachsenen nämlich bei Anzahlen grösser als 4 zunehmend Fehler gemacht. Stattdessen muss also in mühsamer Weise der Vektor dissektiert und die einzelnen Attribute für sich betrachtet werden.

Diese Vektoren scheinen also nicht mehr für Menschen gemacht zu sein.

Doch auch das Erstellen der Vektoren ist mit einem Mehr an Aufwand verbunden. Da, wie wir gleich sehen werden, die Attribute nicht mehr das gleiche Gewicht haben, gestaltet sich das Ausarbeiten von CVSSv4-Vektoren als überaus mühsam. Vor allem dann, wenn gewisse Unbekannten gegeben sind.

## UNWICHTIGE SUBSEQUENT SYSTEM IMPACT METRICS

Grundsätzlich wird in CVSSv4 der Impact in den Vulnerable System Impact Metrics (VSIM) definiert. Diese spezifizieren die Auswirkungen, die das angegriffene System erfährt. Neu wird VC statt C (Confidentiality), VI statt I (Integrity) und VA statt A (Availability) verwendet.

In CVSSv3 wurde das Attribut Scope (S) eingeführt. Es wird herangezogen, um zu deklarieren, ob ein Angriff nur das angegriffene System betrifft (`S:U` für Unchanged) oder ebenfalls Auswirkungen auf andere Komponenten hat (S:C für Changed). In CVSSv4 wird dieses eine Attribut in die Subsequent System Impact Metrics übernommen. Dort kommen nun zusätzlich die Attribute SC (Confidentiality), SI (Integrity) und SA (Availability) zum Tragen:

> The Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the "things that suffer the impact", which may include impact on the vulnerable system and/or the downstream impact on what is formally called the "subsequent system(s)".

Das grundsätzliche Problem ist, dass hier ein enormer Ermessensspielraum vorhanden ist, was nun als unterschiedliche Komponente betrachtet werden soll und inwiefern ein Angriff diese tangieren kann. Ein typisches Beispiel dieser Diskussion ist eine Cross Site Scripting-Schwachstelle in einer Webapplikation. Die Webapplikation ist eigentlich das verwundbare System, bei dem eine Schwachstelle (fehlerhafte Eingabeüberprüfung) ausgenutzt wird.

Traditionellerweise würde der Impact in VSIM als VC:N/VI:L/VA:N definiert werden. Doch effektiv entfalten kann sich die Schwachstelle (Ausführen des injizierten Script-Codes) nur im Webbrowser, der

seinerseits also als Subsequent System verstanden werden kann. Der gleiche Impact-Vektor müsste also mindestens auch in der Form SC:N/SI:L/SA:N übernommen werden.

Doch stimmt das? Schliesslich kann mit einer XSS-Schwachstelle ebenfalls Daten aus dem Browser getragen werden (z.B. Cookies), also gilt es den Vektor mindestens als SC:L/SI:L/SA:N anzupassen. Spätestens wenn der Browser mit administrativen Rechten ausgeführt wird, liesse sich auch darüber diskutieren, dass das Risiko auf SC:H/SI:H/SA:H hochgestuft wird. Der Score würde damit von 6.9 (Medium) auf 7.9 (High) angehoben werden. Ist das wirklich für alle XSS-Angriffe gerechtfertigt?

Laut dem Paradigma von CVSS ist immer vom schlimmstmöglichen Szenario auszugehen. Zudem müssen diese Attribute zwingend ausgefüllt werden. Es sind keine optionalen Attribute, die mit einem Not Defined (X) abgetan werden könnten. Oftmals weiss man jedoch gar nicht, ob und inwiefern die Schwachstelle nun Einfluss auf andere Systeme haben wird. Manchmal auch deswegen, weil es von Konfigurationseinstellungen und individuellen Mechanismen vor Ort abhängt. Deshalb gehören diese Attribute schon fast eher in die Environmental Metrics statt in die Base Metrics.

## UNWIRKSAME SUPPLEMENTAL METRICS

Neu gibt es die Supplemental Metrics, die durch den Supplier des Vektors auszufüllen sind. Diese 6 Attribute sind optional, definieren sie nämlich Eigenschaften wie die Anforderungen an Safety (S), ob ein Angriff automatisierbar ist (AU) und wie die Recovery (R) von einem Angriff auszusehen hat.

Diese Attribute sind nicht nur optional, sie sind nur eine zusätzliche Information und üben keinerlei Einfluss auf den Score aus. Nehmen wir einmal mehr das Beispiel der SQL-Injection, die ihrerseits ein Medizinalgerät mit heiklen Patientendaten betrifft. Der neue Gesamtvektor mit seinen zusätzlichen Anforderungen sähe nun wie folgt aus:

```
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/
VA:L/SC:N/SI:N/SA:N/S:P/AU:Y/R:A/V:C/RE:H/
U:Red
```

Der Score verharrt unverändert bei 6.9, unabhängig ob nun die Supplemental Metrics ausgefüllt werden oder nicht. Einen solch langen Vektor zu erstellen oder ihn zu verstehen setzt intensive Überlegungen voraus. Dass Provider Urgency (U) als einziges Attribut aller verfügbarer Attribute dann auch nicht als einzelner Buchstabe abgekürzt (z.B. U:R), sondern als ganzes Wort U:Red ausgeschrieben wird, ist hierbei wohl das kleinste Problem.

## THREAT METRICS ALS TEMP SCORES

In CVSSv2 und CVSSv3 wurde zwischen verschiedenen Score-Typen unterschieden. Der sogenannte Base Score beinhaltete alle statischen Informationen zu einer Schwachstelle, die für alle Benutzer und über die Zeit hinweg gleich blieben. Der Temp Score baute darauf auf und berücksichtigte zusätzlich Eigenschaften, die sich über die Zeit hinweg ändern, wie zum Beispiel die Verfügbarkeit von Exploits und Gegenmassnahmen. Und der Environmental Score bezog die individuellen Gegebenheiten je nach Kunde und Umgebung mit ein.

CVSSv4 handhabt das zwar im Prinzip ähnlich: Hier wird der Base Score als CVSS-B und der Environmental Score als CVSS-BE dargestellt. Es gibt zwar auch eine Art Temp Score, der als CVSS-BT dargestellt wird, jedoch einen Grossteil der beliebten Eigenschaften gänzlich vernachlässigt. Er wird enger definiert und als Threat Score gehandelt.

Bis anhin wurden nämlich die Report Confidence (RC), das Remediation Level (RL) und die Exploit Code Maturity (E) im Temp Score verwendet. Bei CVSSv4 wird hingegen nur noch die Exploit Maturity (E) (früher Exploitability) berücksichtigt. Diese sieht die Zustände Not Defined (X), Attacked (A), POC (P) und Unreported (U) vor.

Was hier auffällt ist das Ungleichgewicht: Bei POC (P) handelt es sich um den Qualitätszustand eines Exploits und bei Attacked (A) um die bestätigte Handlung von böswilligen Akteuren. Hinzu kommt, dass es in der Regel vom POC (P) zu Attacked (A) nicht lange dauert, denn ein Angreifer mit technischem Verständnis ist in der Regel innert kürzester Zeit in der Lage einen Weaponized Exploit zu entwickeln. Und oftmals ist es halt auch so, dass mit einem

| Metrics | Vektor | Score | Delta | Risiko |
|---|---|---|---|---|
| CVSS-B | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N | 6.9 | ±0 | Medium |
| CVSS-BT Not Defined | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X | 6.9 | ±0 | Medium |
| CVSS-BT Attacked | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:A | 6.9 | ±0 | Medium |
| CVSS-BT POC | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P | 5.5 | -1.4 (20.28%) | Medium |
| CVSS-BT Unreported | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:U | 2.7 | -2.8 (50.9%) | Low |

POC ein Angriff umgesetzt werden kann. Vielleicht ein bisschen unhandlich und nicht vollständig automatisiert, aber ein Ausnutzen vermag durchaus möglich sein.

Diese Threat Metrics sind generell sehr einseitig, besprechen sie in erster Linie die Qualität bzw. die Aktivitäten auf der Angreiferseite:

> This metric measures the likelihood of the vulnerability being attacked, and is based on the current state of exploit techniques, exploit code availability, or active, “in-the-wild” exploitation.

Dies mag für Red Teams interessant sein und Blue Teams zu einem kleinen Teil helfen den aktuellen Stand einzuschätzen. Die Qualität der Veröffentlichung und die Verfügbarkeit von Gegenmassnahmen ist jedoch mindestens so wichtig, um Risiken einschätzen zu können. Dass diese Aspekte einfach ersatzlos verworfen wurden, irritiert.

Hinzu kommt der unliebsame Effekt, dass das Auswählen der Threat Metrics stets einen gravierenden Einfluss auf den Score hat. Bleiben wir bei der SQL-Injection-Schwachstelle in obiger Grafik.

Hierbei fällt auf, dass der maximale Score von 6.9 erreicht wird, wenn entweder CVSS-B verwendet wird oder CVSS-BT mit der schlechtesten Annahme von Attacked. Es wird in diesem Zusammenhang also vom schlimmstmöglichen ausgegangen, sofern nichts anderes bekannt ist.

In den meisten Fällen ist der Zustand aber nicht Not Defined (X) sondern Unreported (U). Es sind also weder Exploits noch Angriffe bekannt. Hier wird aber plötzlich nicht mehr vom schlimmstmöglichen ausgegangen, sondern der Score auf ein 2.7 (Medium) heruntergestuft. Dies entspricht einer totalen Minderung von 4.2 Punkten (60.86%). Ich zweifle daran, dass dieser Widerspruch so gewollt sein kann. Es sei denn, man wollte den Kunden ein Werkzeug in die Hand geben, um die meisten Schwachstellen unkompliziert herunterstufen und damit marginalisieren zu können.

## DOKUMENTATION UND BEISPIELIMPLEMENTIERUNG

In ihren Grundzügen, was Struktur und Ausrichtung betrifft, unterscheiden sich die Dokumentationen der verschiedenen CVSS-Versionen nicht voneinander. Was aber auffällt ist, dass bei CVSSv4 auf die Offenlegung und Darstellung der zugrundeliegenden mathematischen Formeln wie bei CVSSv3 verzichtet wird.

Stattdessen wird auf GitHub nur eine Beispielimplementierung in Javascript zur Verfügung gestellt. Es ist jene Umsetzung, die auch auf dem offiziellen CVSS v4.0 Calculator Verwendung findet. Diese weist einige Sonderheiten auf, die auf einen eigenwilligen Programmierstil zurückzuführen sind (z.B. werden oft komplexe negierte else if-Ausdrücke verwendet, obwohl ein simpler else-Ausdruck genauso möglich gewesen wäre; inkrementierende for-Schleifen werden nachvollziehbaren .forEach-Konstrukten vorgezogen).

Das Portieren und Umsetzen einer eigenen Implementierung gestaltet sich deshalb in CVSSv4 schwieriger, da man nicht auf eine neutrale Darstellung der Funktionsweise zurückgreifen kann. So gibt es auch bis heute nur sehr wenige Portierungen in anderen Sprachen. Zudem gibt es scheinbar Abweichungen, wenn es um das Runden von Werten geht, was im schlimmsten Fall dazu führen kann, dass je nach Implementierung ein anderer Score generiert wird.

## FAZIT

CVSSv4 ist komplex und kompliziert. Das Einführen von zusätzlichen Attributen sollte wohl der Granularität dienlich sein und mit ihr die Präzision erhöhen. Doch zuerst hätte man sich die Frage stellen müssen, ob eine solche überhaupt wünschenswert oder gar erforderlich ist. Die meisten Nutzer von CVSS interessieren sich entweder sowieso nur für die Scores, ohne die Vektoren im Detail anzuschauen. Oder sie lieben es unendlich lange darüber zu philosophieren, welcher Vektor nun wirklich das richtigste Szenario widerzuspiegeln in der Lage ist:

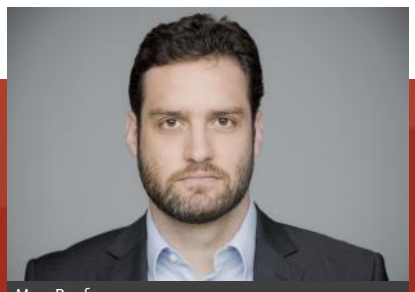
> It is likely that many different types of individuals will be assessing vulnerabilities (e.g., software vendors, vulnerability bulletin analysts, security product vendors), however, note that CVSS assessment is intended to be agnostic to the individual and their organization.

Diese Diskussion kann sich nun auch über die verschiedenen Generationen von CVSS erstrecken, denn die zu Beginn ins Feld geführte SQL-Injection ist je nachdem eine 7.5 (CVSSv2), 7.3 (CVSSv3) oder 6.9 (CVSSv4). Die Genauigkeit von CVSS ist also generell nicht gegeben, weshalb ein Mehr an Komplexität nur über die Probleme hinwegtäuscht und zusätzliche Nachteile mit sich bringt.

Das Verkümmern der Temp Scores ist zudem eine absolute Fehlentscheidung. Ein Grossteil der CVSS-Anwender – gerade Administratoren und Blue Teams – orientiert sich massgeblich an diesen Attributen. Durch das Weglassen eben dieser wird die Nützlichkeit der Metrik für diese Nutzergruppe in absoluter Weise gemindert. Aus diesem Grund kann ich mir nicht vorstellen, dass sich CVSSv4 bei der breiten Masse durchsetzen können wird. Es müsste eine zusätzliche Metrik eingeführt werden, um das neu mitgebrachte Unvermögen wieder kompensieren zu können.

Ich bin der Meinung, dass sich CVSSv4 nicht reparieren lässt. Zwar werden voraussichtlich einige kleinere Mängel in einer Version 4.1 adressiert werden. Es sind jedoch bei der Ausarbeitung einige grundlegende Entscheidungen gefällt worden, deren Verbesserung ein komplettes Überarbeiten der Metrik erzwingen würde. Die Kompatibilität eines Minor-Releases würde dadurch gänzlich verloren gehen. Es bleibt also zu hoffen, dass mit CVSSv5 alles besser wird. Ein bisschen weniger Komplexität täte dem Ansatz definitiv wieder gut.

Die ersten Newsartikel und Beiträge zu CVSSv4 waren alle sehr optimistisch. Als aufmerksamer Leser hat man jedoch schnell gemerkt, dass die Autoren sich nicht mit den Details auseinandergesetzt oder die neue Metrik (produktiv) eingesetzt haben. Ich kann mir nur vorstellen, dass sich CVSSv4 durchsetzen kann, wenn auch weiterhin die Details der Metrik vernachlässigt und sich blindlings auf die Scores verlassen wird. Ich muss gestehen, dass das eine meiner grössten Befürchtungen ist. Denn in diesem Fall würde undankbarerweise CVSS zu einer Farce verkommen.


Marc Ruef

# Künstliche Intelligenz: Wie wir das Thema aus Sicherheitsperspektive behandeln

Künstliche Intelligenz ist eine Thematik, die uns aktuell mehr denn je herausfordert. Wir von der scip AG beschäftigen uns in diversen Projekten und Forschungsaufträgen mit der Nutzung von künstlichen Systemen. Dabei schaffen wir den Spagat zwischen gesellschaftlichen und ethischen Bedingungen, und kreieren einen nachhaltigen Mehrwert im Umgang mit der Technologie. Als Security Unternehmen betrachten wir KI auch mit kritischen Augen und pflegen einen achtsamen und sinnstiftenden Umgang damit.

## WIE WIR UNTERSTÜTZEN

Gemeinsam erarbeiten wir die Grundlagen, dies kann in Form einer Projektbegleitung oder im Rahmen eines Workshops stattfinden. Es kann aber auch ein umfangreiches Fachdokument entstehen, das die essentiell wichtigen Punkte zusammenfasst. Wir unterstützen in den Bereichen Analyse von Deepfakes, Ethik, Vertrauen & Interaktion, IQ Bewertung und Sprachanalyse, OSINT Recherche von Bildern, Informationen & Geodaten, Digitalisierung & Einsatzbereiche GenAI.

https://www.scip.ch/?artificial_intelligence

Bilderquelle: https://unsplash.com/de/fotos/vollmond-tagsuber-yOIT88xWkbg

ERIC MAURER

# ACTIVE DIRECTORY ZERTIFIKATSDIENSTE: ANGRIFF UND VERTEIDIGUNG

Microsoft Active Directory Public Key Infrastructure (PKI), besser bekannt als Active Directory Certificate Services (AD CS), ist eine Windows Server Rolle zur Ausstellung und Verwaltung von PKI-Zertifikaten, die in sicheren Kommunikations- und Authentifizierungsprotokollen verwendet werden. Diese Zertifikate können zur Verschlüsselung und Signatur von Dokumenten und Nachrichten sowie zur Authentifizierung von Computer- und/oder Benutzerkonten verwendet werden. In diesem Beitrag werden wir einen genaueren Blick auf die Fehlkonfigurationen werfen und wie wir sie nutzen können, um Active Directory-Umgebungen anzugreifen. Die Möglichkeiten reichen vom Diebstahl von Anmeldeinformationen über die Persistenz von Rechnern bis hin zur Domäneneskalation. Die Techniken basieren auf dem Certified Pre-Owned Whitepaper von Will Schroeder und Lee Christensen.

Ziel dieses Beitrags ist es, eine kurze Einführung in dieses komplexe und offen gesagt manchmal etwas trockene, aber sehr wichtige Thema zu geben. Wir werden einige grundlegende Funktionen behandeln, wie Zertifikate aussehen und wie sie ge- und missbraucht werden können.

## ÜBERSICHT

AD CS kann entweder als Standalone Certificate Authority (CA) oder als Enterprise CA eingesetzt werden. Eine Standalone CA verfügen nicht über Funktionen wie Zertifikatsvorlagen und AutoEnrollment, weshalb sie eher als Root- und Policy-CAs eingesetzt werden und nur Zertifikate für andere CAs ausstellen. Die Enterprise CA verfügt über Funktionen wie Zertifikatsvorlagen und AutoEnrollment, die in den meisten Fällen für Unternehmensumgebungen entscheidend sind. Was sind diese Funktionen und wie funktionieren sie?

- Zertifikatsvorlagen können als Blaupausen mit vordefinierten Einstellungen für Zertifikate betrachtet werden. Die Einstellungen definieren Dinge wie Wofür wird das Zertifikat verwendet, Wer kann ein Zertifikat beantragen, Wie lange ist das Zertifikat gültig und so weiter. Je nach Verwendung eines Zertifikats können die Einstellungen in diesen Blaupausen angepasst werden.

- AutoEnrollment ermöglicht es Clients (Benutzern und Computern), automatisch Zerti-

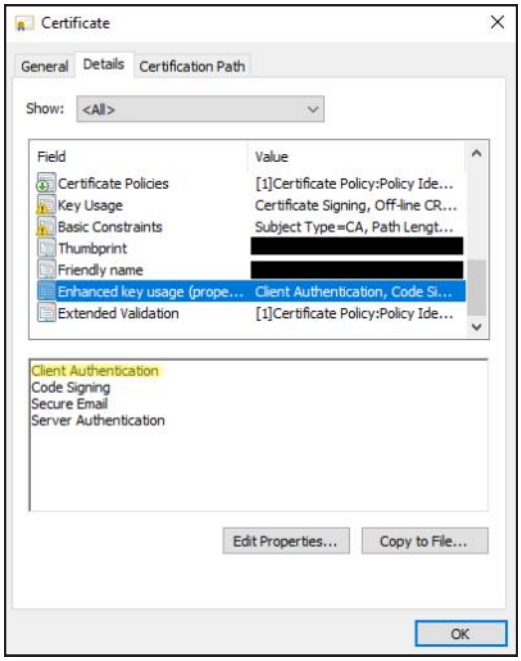
fikate in einer Active Directory-Domäne auf der Grundlage vordefinierter Zertifikatsvorlagen anzufordern und zu erhalten.

## ZERTIFIKATE

Wie bereits erwähnt, enthält ein Zertifikat verschiedene Felder mit Informationen darüber, wie und wofür das Zertifikat verwendet werden soll. Schauen wir uns einige dieser Felder und die erwarteten Werte genauer an:

- Seriennummer: Kennung für ein von der Zertifizierungsstelle zugewiesenes Zertifikat
- Issuer: Gibt an, wer das Zertifikat ausgestellt hat, normalerweise eine Zertifizierungsstelle
- Gültig von und Gültig bis: Gibt das Datum an, ab dem das Zertifikat gültig ist, bis es abläuft
- Subject: Eigentümer des Zertifikats
- Enhanced Key Usages: Auch bekannt als Extended Key Usages (EKUs) – Objektbezeichner (OIDs) beschreiben, wofür das Zertifikat verwendet werden kann.

Die im Zertifikat enthaltenen Informationen binden eine Identität – das Subject – an das Schlüsselpaar.



EKUs und OIDs stehen in Beziehung zueinander, eine OID ist im Grunde eine Kette von Dezimalzahlen, die ein Objekt eindeutig identifiziert. Im Moment sind die EKUs, die die Authentifizierung bei AD ermöglichen, interessant und wir konzentrieren uns auf folgende:

| EKU Wert | OID |
|---|---|
| Client-Authentifizierung | 1.3.6.1.5.5.7.3.2 |
| Smart Card-Anmeldung | 1.3.6.1.4.1.311.20.2.2 |
| Beliebiger Zweck | 2.5.29.37.0 |

Weitere Informationen über OIDs in PKI finden Sie in diesem PKI Solutions Post.

## ZERTIFIKATSREGISTRIERUNG

Nach der Installation der AD CS-Rolle als Enterprise CA muss ein Administrator zunächst Zertifikatsvorlagen erstellen und definieren. Diese werden dann von der Enterprise CA veröffentlicht und den Benutzern und Computern zur Registrierung zur Verfügung gestellt. Ohne zu sehr ins Detail zu gehen, ein Client kann nur dann ein Zertifikat anfordern, wenn er sowohl auf der Enterprise CA als auch in der Zertifikatsvorlage selbst berechtigt ist, ein solches Zertifikat zu beantragen. Weitere technische Informationen darüber, wie diese Berechtigungen festgelegt werden, können im Whitepaper im Kapitel Certificate Enrollment gefunden werden.

Wenn die Berechtigungen erteilt sind und ein Client ein Zertifikat anfordern darf, kann dies je nach AD CS-Umgebung auf unterschiedliche Weise geschehen:

- Mit dem Windows Client Certificate Enrollment Protocol (MS-WCCE).
- Mit dem ICertPassage Remote Protocol (MS-ICPR).
- Über eine Web-Enrollment-Anwendung, dazu muss auf dem AD CS Server die Rolle Certificate Authority Web Enrollment installiert sein.

| Technik | Beschreibung |
|---|---|
| Diebstahl | Stehlen, Extrahieren und Exportieren bereits ausgestellter Computer- oder Benutzerzertifikate und privater Schlüssel. Dies geschieht mit Window's Crypto APIs, DPAPI und PKINIT |
| Persistenz | Kontopersistenz über Authentifizierungszertifikate für einen Benutzer und/oder Computer |
| Eskalation | Domänen-Eskalation über anfällige/fehlkonfigurierte AD CS-Komponenten. Dazu gehören falsch konfigurierte Zertifikatsvorlagen, AD-Objekte und Zertifikatsregistrierungsoptionen. |
| Domänenpersistenz | Möglichkeit, Domänenpersistenz über Zertifikatsfälschung zu erreichen, entweder durch gestohlene private CA-Schlüssel, bösartige Zertifikate oder Fehlkonfigurationen |

- Über den Certificate Enrollment Service (CES), hierfür muss auf dem AD CS Server die Rolle Certificate Enrollment Web Service installiert sein.

- Über den Network Device Enrollment Service, hierfür muss auf dem AD CS Server die Rolle Network Device Enrollment Service installiert sein.

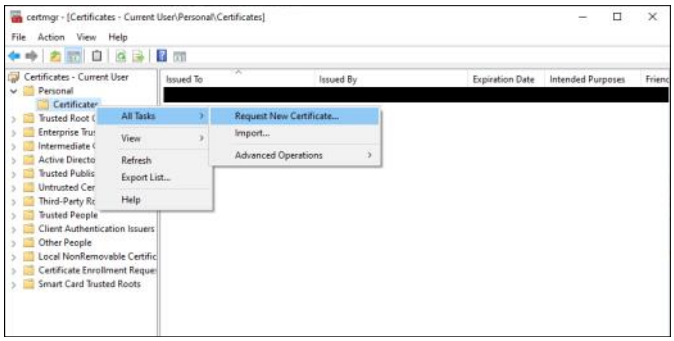
Ein Beispiel: Ein Benutzer muss manuell ein neues Zertifikat für seinen Windows-Rechner anfordern. Der erste Schritt besteht darin, die grafische Benutzeroberfläche zu öffnen, indem certmgr.msc (certlm.msc für Computerzertifikate) in das Suchfeld von Windows eingeben wird. Öffnen Sie den Ordner Persönlich, klicken Sie mit der rechten Maustaste auf den Ordner Zertifikate und wählen Sie Alle Aufgaben, Neues Zertifikat anfordern.

Nun öffnet sich ein weiterer Assistent und alle veröffentlichten Zertifikatsvorlagen, die der Benutzer anfordern darf, werden angezeigt und können angefordert werden. Standardmässig fordert Windows dann das Zertifikat mit MS-WCCE an.

## OFFENSIVTECHNIKEN

Die Angriffstechniken werden in vier verschiedene Kategorien, basierend auf den verschiedenen Angriffstechniken aus dem Whitepaper, unterteilt: Diebstahl, Persistenz, Eskalation und Domänenpersistenz. Die obige Tabelle hilft, die Unterschiede zwischen den Kategorien zu verstehen.

Um zu verstehen, welche Techniken in diesen Kategorien enthalten sind, sehen wir uns eine der Eskalations-Möglichkeiten an, wenn AD CS falsch konfiguriert ist.



### NTLM-RELAY ZU EINEM ANFÄLLIGEN AD CS HTTP-ENDPUNKT (ESC8)

Wie im Kapitel Zertifikatsregistrierung erwähnt, stehen mehrere HTTP-basierte Schnittstellen für die Zertifikatsregistrierung zur Verfügung, sofern sie installiert sind. Diese HTTP-Schnittstellen sind im Allgemeinen anfällig für NTLM-Relay-Angriffe. Ein Angreifer auf einem kompromittierten Rechner könnte die Net-NTLMv2-Authentifizierung manipulieren und sich als dieses AD-Konto ausgeben, um Zugriff auf Zertifikatsanforderungen zu erhalten oder andere Operationen im Namen des Benutzers durchzuführen. Dies könnte zu Sicherheitsproblemen wie unbefugtem Zugriff und der Ausstellung nicht autorisierter Zertifikate führen.

Gehen wir einen möglichen Angriff durch, bei dem AD CS für ESC8 anfällig ist:

- Einem Angreifer gelingt es, einen Rechner eines Endbenutzers zu kompromittieren und auf diesem Fuss zu fassen.
- Nach einer ersten Erkundung des Active Directory wurde die ESC8-Schwachstelle mit Hilfe des Tools Certify in der Active Directory Certificate Service Rolle identifiziert.
- Um den Angriff auf die AD CS-Webschnittstelle zu starten, muss sich ein Opfer am vom Angreifer kontrollierten Client authentifizieren, um den NTLM-Relay-Angriff zu starten. Bei diesem Beispiel gehen wir davon aus dass eines der folgenden Szenarien eingetreten ist:

- Der Angreifer hat genügend Zeit und kann darauf warten, dass dies als Teil des Tagesgeschäfts im Netzwerk geschieht.

- Der Angreifer schafft es, ein Konto zu zwingen, sich gegenüber dem vom Angreifer kontrollierten Rechner zu authentifizieren. Bevorzugte Ziele sind Domänencontroller und/oder hochprivilegierte Konten.

- Nachdem ein Domänencontroller erfolgreich dazu gebracht wurde sich bei dem vom Angreifer kontrollierten Rechner zu melden, wird der NetNTLMv2-Hash des DC mitgesendet und kann danach an den AD CS HTTP-Endpunkt weitergeleitet werden.

- Da der HTTP-Endpunkt keinen Relay-Schutz hat, kann der Angreifer Zertifikate im Namen des ursprünglichen Absenders, in diesem Fall des Domänencontrollers, anfordern.

- Nun wird ein Zertifikat ausgestellt, das auf einer Zertifikatsvorlage mit geeigneten Enhanced Key Usage Werten wie Client Authentication oder SmartCard Logon basiert.

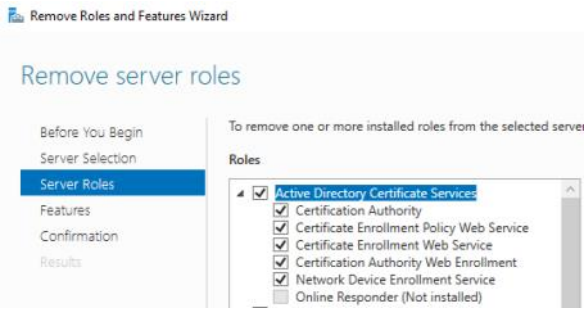
- Da der betroffene Computer ein Domänencontroller war, der hochprivilegierte Aktionen wie Domänenreplikation durchführen kann, könnte der Angreifer das Zertifikat verwenden, um die Domäne zu kompromittieren. Einige der Möglichkeiten wären zum Beispiel der Versuch, einen DCSync-Angriff auszuführen, den NTHash oder ein Kerberos Ticket Granting Ticket (TGT) über PKINIT zu erhalten.

## DEFENSIVTECHNIKEN

Wenn die Angriffstechniken bekannt sind, ist es etwas einfacher, sich gegen sie zu schützen. Will Schroeder und Lee Christensen haben diese Abwehrtechniken bereits nummeriert und kategorisieren diese defensiven Techniken in präventive und detektive Massnahmen. Das Tool PSPKIAudit kann zur Auflistung von fehlkonfigurierten Vorlagen verwendet werden. Nach der Identifizierung von Fehlkonfigurationen ist es empfehlenswert, sich mit den Defensivtechniken zu befassen und den Abschnitt Defensive Guidance zu befolgen, um sie entsprechend zu verwalten. Wir werden nicht auf die verschiedenen Kontrollen eingehen und wie sie den offensiven Techniken zugeordnet werden, da dies im Whitepaper gut beschrieben ist, ich möchte jedoch kurz auf die Präventivmassnahmen gegen die ESC8-Schwachstelle eingehen.

## AD CS HTTP-ENDPUNKTE HÄRTEN (PREVENT8)

Die effektivste Methode, um die ESC8-Schwachstelle zu verhindern, besteht darin die AD CS HTTP-Endpunkte gar nicht erst zu aktivieren. Um zu ermitteln welche Endpunkte aktiviert sind, und sie zu entfernen, verbinden Sie sich mit dem Server, auf dem die AD CS-Rolle ausgeführt wird, öffnen Sie die App Server Manager und verwenden Sie den Assistenten Rollen und Funktionen entfernen.



Wenn die Endpunkte notwendig sind und es nicht möglich ist, sie zu entfernen, könnten diese Abwehrmassnahmen gegen ESC8 in Betracht gezogen werden.

- Deaktivieren Sie die NTLM-Authentifizierung, die Deaktivierung von NTLM kann auf der Ebene des Hosts oder des Webservers (Internet Information Services (IIS)) vorgenommen werden.

- Erzwingen Sie HTTPS auf IIS-Ebene, aktivieren Sie Erweiterter Schutz für die Authentifizierung und setzen Sie den Wert Erweiterter Schutz auf Erforderlich.

## ZUSAMMENFASSUNG

Active Directory Certificate Services können sehr schnell komplex werden und sind in den meisten Umgebungen nicht einfach zu implementieren und zu sichern. Die verschiedenen Möglichkeiten, wie AD CS konfiguriert, erweitert und für verschiedene Anwendungsfälle angepasst werden kann, machen es schwer, dies effektiv abzusichern. Die verschiedenen Techniken des Zertifikatsmissbrauchs ermöglichen Angreifern in kurzer Zeit von Credential Theft über Domain Persistence bis hin zu Domain Escalation zu gelangen. Die erwähnten Tools Certify (AD CS Enumeration) und PSPKIAudit (Auditing AD CS) eignen sich hervorragend, um etwaige Schwachstellen in der Infrastruktur aufzuzeigen, die dann behoben werden können. Falls noch nicht geschehen, empfiehlt es sich, die AD CS-Umgebung und die Zertifikatsvorlagen kontinuierlich zu überprüfen. Zusammengefasst: Nicht nur die Domänencontroller müssen geschützt werden, sondern auch die CA-Server, behandeln Sie sie wie ein Tier 0 System.

Eric Maurer




Bildquelle: https://unsplash.com/de/fotos/brown-mountain-under-starry-sky-7Ym9rpYtSdA

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



## 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.



scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch