MONTHLY SECURITY SUMMARY

AUSGABE FEBRUAR 2024
LERNEN AUS FEHLERN & RICHTIG DOKUMENTIEREN

VON DER KRISE ZUR CHANCE

Wir zeigen, wie sich Lerneffekte positiv auf die Cyber-Resilienz auswirken und unterstützen mit Leitlinien hinsichtlich Cybersicherheitsvorfällen.

WIESO DOKUMENTIEREN SO WICHTIG IST

Dokumentieren in der Cybersicherheit? Unbedingt! Wir legen dar, wieso das Erstellen von gut dokumentierten Reports zum Security Testing dazugehört.

Februar 2024: Sicherheit, überall.

Februar ist Pistenzeit!

Zumindest ist es bei uns im Wallis so. Die meisten Schulen und Bildungseinrichtungen führen während dieser Zeit eine unterrichtsfreie Phase ein, damit ihren wintersportlichen Aktivitäten nachgegangen werden kann. Ich erinnere mich noch gut an meine Schulzeit. Meistens unternahmen wir mit der gesamten Klasse Skiausflüge auf den Rosswald, oder fuhren mit dem Postauto in das weitaus grössere Gebiet, auf die Belalp hinauf. Fast vollgepackt rasten wir die Pisten hinunter, unsere Rucksäcke prallgefüllt mit Sandwiches, Süssigkeiten und Tee. Mit reichlich Schnee, aber dafür ohne Schutz. In meiner Kindheit war das Tragen von Helmen nämlich noch kein Thema.

Heutzutage kann man sich das kaum noch vorstellen: Eine Ski– oder Snowboardfahrt ohne Schutzhelm? Wir haben damals von unseren Fehlern gelernt, und setzen mittlerweile auch beim Wintersport auf mehr Sicherheit. In der digitalen Welt sollte es nicht anders sein, und dennoch sind im Jahre 2024 viele Unternehmen, Gesundheitseinrichtungen aber auch Privatpersonen ziemlich schutzlos unterwegs, wenn es um Cybersicherheit geht.

Lassen Sie uns also wieder mehr Wert auf Security-Themen legen, sei es beim Pistengang oder im Umgang mit dem Internet. Und auch das mit dem Schnee liegt in unserer Hand, wenn wir unsere Berge und Natur schützen und wertschätzen.

Sichere Fahrt!

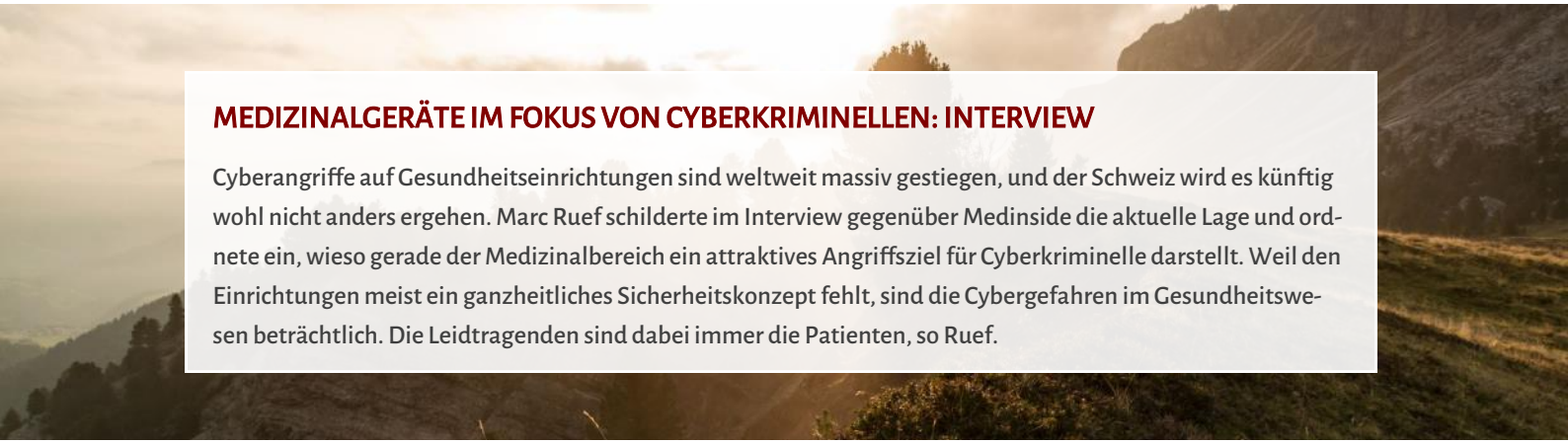
Serena Bolt
Research Team

NEWS

WAS IST BEI UNS PASSIERT?

KI IN DEN SOZIALEN MEDIEN: BEITRAG AUF 20 MINUTEN

Der Einsatz von künstlicher Intelligenz in den Sozialen Medien wird bereits seit längerer Zeit diskutiert. Im Beitrag von 20 Minuten erklärte Marisa Tschopp, wie KI-generierter Content in den Sozialen Medien erkannt werden kann. Tschopp sagte dabei, dass es aktuell eher schwierig sei, zuverlässige Detektoren zu entwickeln, die den Unterschied zwischen menschlich und technisch generierten Inhalten erkennen können. Wichtig sei dabei eine kritische Auseinandersetzung mit den Möglichkeiten und Grenzen von KI.



MEDIZINALGERÄTE IM FOKUS VON CYBERKRIMINELLEN: INTERVIEW

Cyberangriffe auf Gesundheitseinrichtungen sind weltweit massiv gestiegen, und der Schweiz wird es künftig wohl nicht anders ergehen. Marc Ruef schilderte im Interview gegenüber Medinside die aktuelle Lage und ordnete ein, wieso gerade der Medizinalbereich ein attraktives Angriffsziel für Cyberkriminelle darstellt. Weil den Einrichtungen meist ein ganzheitliches Sicherheitskonzept fehlt, sind die Cybergefahren im Gesundheitswesen beträchtlich. Die Leidtragenden sind dabei immer die Patienten, so Ruef.

DIE KRAFT DER UNZUFRIEDENHEIT: KI EVENT

KI macht unzufrieden, weil sie uns nur durchschnittlich macht: Diese These wird am 29. Februar 2024 unter anderem mit Marisa Tschopp an der Artificial Intelligence Edition in Zürich diskutiert. Marisa Tschopp, die die Technologie aus psychologischer Sicht erforscht, wird gemeinsam mit anderen Expertinnen und Experten aus der Community auf der Bühne zu sehen sein. Der Anlass findet für geladene Gäste statt.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

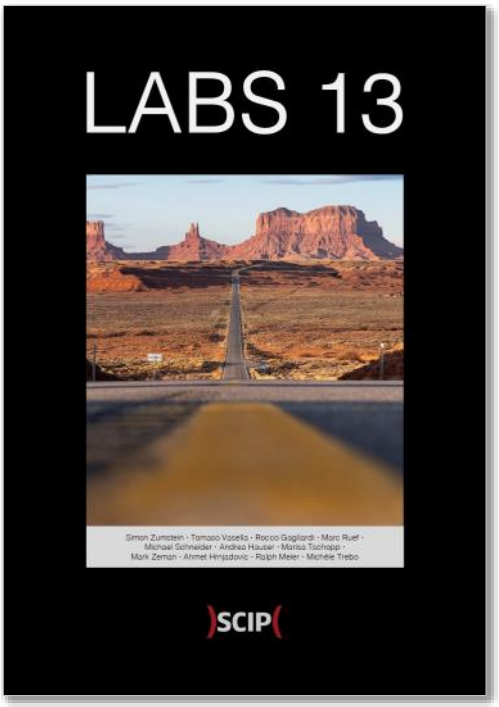
UNSER AKTUELLES JAHRBUCH

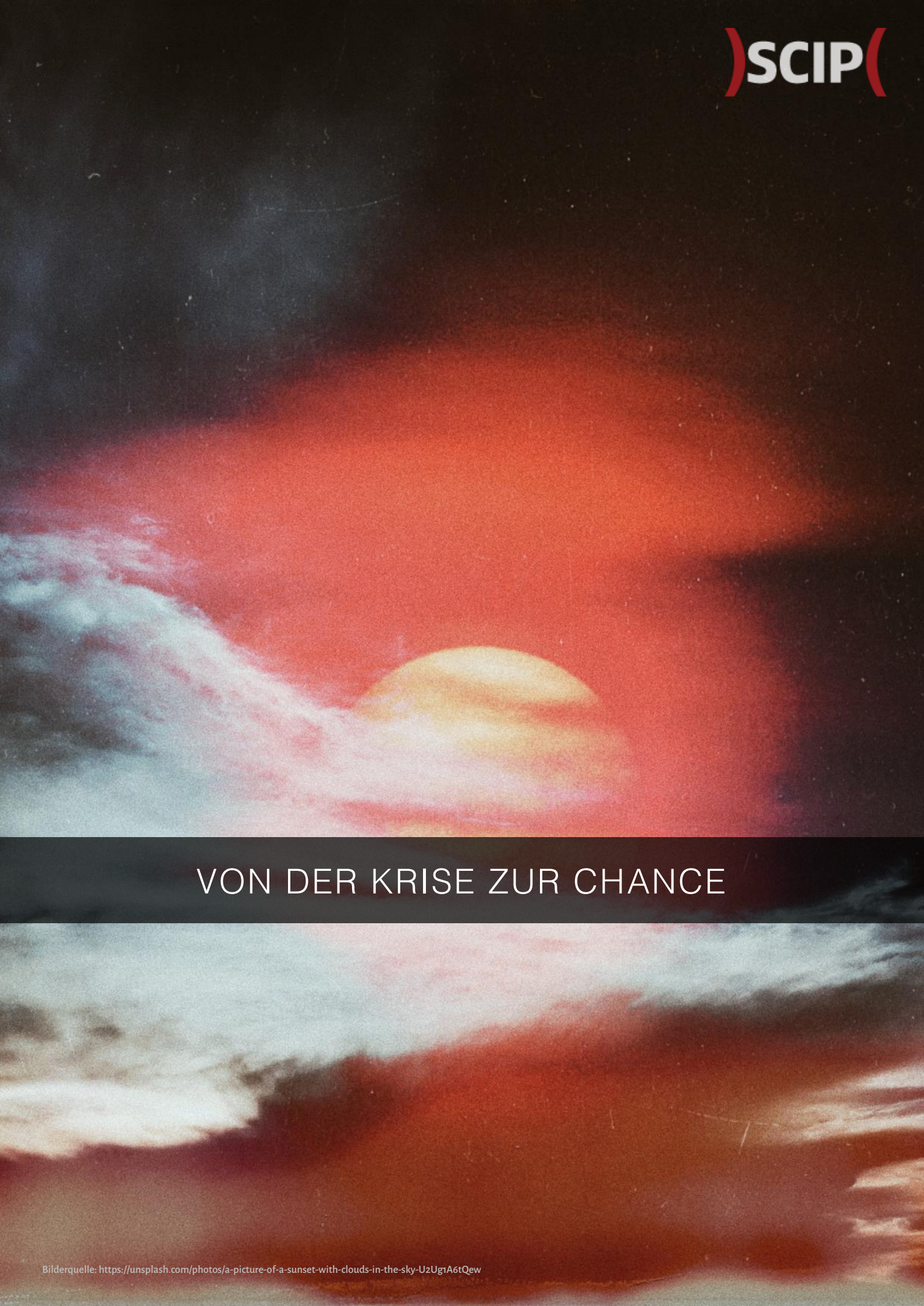
Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

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.





VON DER KRISE ZUR CHANCE

Bilderquelle: https://unsplash.com/photos/a-picture-of-a-sunset-with-clouds-in-the-sky-U2Ug1A6tQew

MICHÈLE TREBO

VON DER KRISE ZUR CHANCE: LERNEN AUS FEHLERN

Cybersicherheitsvorfälle rücken immer stärker in den Fokus des Risikomanagements von Unternehmen. Um effektiv auf die sich stetig entwickelnden Bedrohungen reagieren zu können und die Cyber-Resilienz zu verbessern, ist es entscheidend, Cybersicherheitsvorfälle zu analysieren und daraus zu lernen. Dieser Artikel fasst die Studie „*I don't think we're there yet: The practices and challenges of organisational learning from cyber security incidents*" zusammen und versucht darauf basierend Leitlinien für Schweizer Unternehmen abzuleiten.

ÜBERBLICK

Die rasanten Entwicklungen digitaler Technologien haben Unternehmen ermöglicht, ihre betriebliche Effizienz zu steigern und Kosten zu senken. Allerdings sind diese Vorteile mit zunehmenden und sich ständig weiterentwickelnden Cyberbedrohungen verbunden. Die herkömmliche Vorstellung von organisatorischer Verteidigung ist veraltet, da Unternehmen heute in einem dynamischen Ökosystem agieren, das von fliessenden Grenzen und komplexen Lieferantenbeziehungen geprägt ist. Die Integration neuer digitaler Technologien in bestehende IT-Infrastrukturen erhöht die Cybersicherheitsrisiken, da Angriffsflächen für Cyberangriffe wachsen. Dies unterstreicht die Notwendigkeit, die Cybersicherheitsfähigkeiten kontinuierlich zu verbessern. Die weltweite Zahl der Cyberangriffe nimmt zu und die Kosten und Auswirkungen sind erheblich. Cyberangriffe werden als eine der grössten Bedrohungen für Unternehmen angesehen. Der Mangel an qualifizierten Cybersicherheitsexperten erfordert, dass Organisationen effektivere Wege finden, um Sicherheitsvorfälle zu reduzieren. Cybersicherheitsvorfälle können Unternehmen als Lerngelegenheit dienen, um ihre Abwehrkräfte zu stärken und sich vor zukünftigen Bedrohungen zu schützen.

FORSCHUNGSMETHODEN

In der Studie wurde ein qualitativer Ansatz gewählt. Dieser Ansatz ermöglichte ein tiefes Verständnis des Phänomens und berücksichtigte sowohl positivistische als auch konstruktivistische theoretische Rahmenbedingungen. Das Ziel der Studie war es, die Praktiken zu verstehen und zu analysieren, die Organisationen anwenden, um aus Cybersicherheitsvorfällen zu lernen. Die Ergebnisse der Studie wurden in

verallgemeinerter und anonymisierter Form präsentiert und boten aggregierte Erkenntnisse aus mehreren Quellen. Um Einblicke in die Lernpraktiken von Organisationen zu gewinnen, wurden Interviews mit 34 Sicherheitsexperten aus verschiedenen Branchen im Vereinigten Königreich durchgeführt. Die Auswahl der Teilnehmer erfolgte gezielt, um sicherzustellen, dass sie über ausreichende Kenntnisse darüber verfügen, wie ihre Organisation aus Cybersicherheitsvorfällen lernt. Es wurden sowohl virtuelle als auch persönliche Interviews durchgeführt, die aufgezeichnet und transkribiert wurden. Die Codierung und Analyse der Interviews zielte darauf ab, vorherrschende Muster und signifikante Erkenntnisse der Befragten zu identifizieren.

ERKENNTNISSE

Die neoinstitutionelle Theorie hat einen signifikanten Einfluss auf die Entwicklung von Lernpraktiken in Organisationen, insbesondere im Kontext von Cybersicherheitsvorfällen. Sie beeinflusst die Art und Weise, wie Organisationen aus solchen Vorfällen lernen.

ISOMORPHER DRUCK

Gemäss der neoinstitutionellen Theorie neigen Organisationen dazu, unter dem isomorphen Druck ähnliche Praktiken wie andere Organisationen in ihrer Umgebung zu übernehmen, um als legitim und akzeptabel angesehen zu werden. Sie orientieren sich an den Standards und Erwartungen anderer Unternehmen, um ihre eigenen Lernprozesse zu gestalten. Die Befragten gaben an, dass ihre Organisationen die Effektivität der Lernpraktiken nicht explizit bewertet. Das Fehlen wiederholter Vorfälle wurde allerdings als ein Indikator für erfolgreiches Lernen genannt.

ZWANGSMASSNAHMEN

Zwangsmassnahmen spielen eine entscheidende Rolle bei der Gestaltung von Kommunikationspraktiken und der Einbindung von Rechts- und Kommunikationsteams bei der Reaktion auf Cybersicherheitsvorfälle. Die Herausforderungen in diesem Bereich resultieren oft aus der globalen Struktur von Organisationen, da die Zuständigkeit aufgrund verschiedener Faktoren wie dem betroffenen Subjekt, dem Ort

des Vorfalls und der Identität des Angreifers schwer zu bestimmen ist. Darüber hinaus erhöht die Notwendigkeit, mit verschiedenen Aufsichtsbehörden und Regierungsorganisationen zu kommunizieren, die Komplexität der Kommunikation bei einem konkreten Cybersicherheitsvorfall erheblich. Ein weiterer Aspekt, der in der Studie hervorgehoben wird, ist, dass viele Organisationen zwar vertragliche Verpflichtungen für ihre Lieferanten eingeführt haben, die diese dazu verpflichten, Cybersicherheitsvorfälle zu melden, aber die Meldungen meist nicht transparent genug sind. Die Angst vor rechtlichen Konsequenzen und behördlichen Massnahmen schränkt oftmals die Bereitschaft ein, detaillierte Informationen über Cybersicherheitsvorfälle mit anderen Organisationen zu teilen. Dies erschwert das Lernen aus solchen Vorfällen erheblich. Eine offene Kommunikation könnte nicht nur dazu beitragen, besser auf Cybersicherheitsvorfälle zu reagieren, sondern sich auch vor diesen zu schützen.

NORMATIVER DRUCK

Es wurde festgestellt, dass obligatorische Schulungen zur Meldung von Cybersicherheitsvorfällen existieren, aber es keine einheitliche Bewertung ihrer Wirksamkeit gibt. Einige Organisationen ergänzen diese Schulungen durch zusätzliche Ermutigung, um eine Kultur ohne Schuldzuweisungen zu schaffen. Die Klassifizierung von Vorfällen variiert von Organisation zu Organisation und es gibt keine einheitliche Methode. Dies führt zu Herausforderungen bei der Standardisierung und erschwert die Erstellung verlässlicher Statistiken über Cybersicherheitsvorfälle.

MIMETISCHER DRUCK

Rechtliche Bedenken, regulatorische Auswirkungen und vertragliche Verpflichtungen sind wie bereits erwähnt, oft Hindernisse für die detaillierte Weitergabe von Informationen zu Cybersicherheitsvorfällen. Organisationen neigen dazu, Praktiken anderer Organisationen zu imitieren, da die Führung oft ein begrenztes Verständnis für Cyberrisiken hat und der Bereich sich ständig weiterentwickelt. Die Entfernung zwischen einem anderen Cybersicherheitsvor-

fall und der eigenen Organisation beeinflusst die Bereitschaft der Befragten, sich mit diesen fremden Vorfällen auseinanderzusetzen. Dennoch erkennen sie an, dass die Erkenntnisse aus anderen Cybersicherheitsvorfällen die Wahrnehmung der Bedrohungen für die eigene Organisation beeinflusst.

ERKENNUNG VON CYBERSICHERHEITSVORFÄLLEN

Die Befragten gaben an, sich bewusst zu sein, dass es nur eine Frage der Zeit sei, bis ein schwerwiegender Cybersicherheitsvorfall eintreten könnte, wenn sie nicht bereits einen solchen erlebt hatten. Dieses Bewusstsein motiviert sie dazu, proaktiv nach potenziellen Problemen zu suchen und betont die Bedeutung der frühzeitigen Identifizierung von Vorfällen. Die Mehrheit der Befragten betonte die Notwendigkeit eines Arbeitsumfelds, das Cybersicherheitsvorfälle als Chancen für Wachstum und Verbesserung ansieht, anstatt sie als Gelegenheiten für persönliche Entwicklung oder zum Schaden anderer zu betrachten. Es wurde jedoch auch festgestellt, dass die Schaffung einer Kultur der Offenheit und Transparenz erhebliche Herausforderungen mit sich bringt und nicht über Nacht umsetzbar ist.

ERMITTLUNG VON URSACHEN

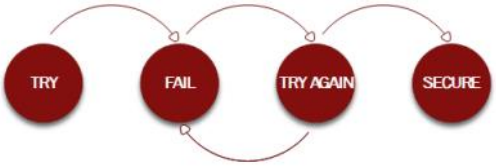
Praktische Einschränkungen wie begrenzter Zeit und Ressourcen erschweren es, Ursachen gründlich zu erforschen. Die Befragten geben zudem an, dass es herausfordernd sei, die Teams dazu zu motivieren, die Untersuchung der zugrunde liegenden Ursachen als Priorität zu behandeln. Die Qualität der Untersuchungen sei stark von der Beteiligung der richtigen Personen zur richtigen Zeit abhängig. Des Weiteren wurden die Unternehmenspolitik und die individuelle Abwehrhaltung als erhebliche Hindernisse bei der Ermittlung der Ursachen identifiziert. Diese Herausforderungen verdeutlichen die Komplexität der Ermittlung von Ursachen von Cybersicherheitsvorfällen und unterstreichen die Bedeutung einer kulturellen Veränderung, angemessener Ressourcenallokation und Fähigkeiten zur Trendanalyse, um die Wirksamkeit von Vorfalluntersuchungen und Lernprozessen innerhalb von Organisationen zu verbessern. Das vollständige Verständnis der Ursachen eines Cybersicherheitsvorfalls ist entscheidend, um daraus zu lernen und die Sicherheit der Organisation zu verbessern.

UMSETZUNG DER AUS VORFÄLLEN GEWONNENEN ERKENNTNISSE

Es gibt Unterschiede in der Art und Weise, wie Organisationen die Umsetzung von Erkenntnissen aus Cybersicherheitsvorfällen verfolgen und wer dafür verantwortlich ist. In einigen regulierten Branchen gibt es strengere Berichtsmechanismen und Risikoausschüsse, die den Fortschritt bei der Umsetzung überwachen, während in anderen Organisationen die Verantwortung oft nach Erstellung eines Vorfallberichts endet. Die Umsetzung der gewonnenen Erkenntnisse kann mit der Zeit nachlassen, da die Energie und Konzentration während eines Cybersicherheitsvorfalls abnehmen und andere Aufgaben dringender werden. Strukturelle Probleme und grössere Investitionen können ebenfalls dazu führen, dass solche Massnahmen hinausgezögert werden. Einige Organisationen übersehen Lernmöglichkeiten aus Cybersicherheitsvorfällen. Andere nutzen sie jedoch, um Aufmerksamkeit und Finanzierung für Sicherheitsinitiativen zu gewinnen. Es ist notwendig, robuste Mechanismen zur Verfolgung von Erkenntnissen und zur Aufrechterhaltung der Umsetzungsdynamik zu etablieren, strategische Investitionen zu priorisieren und regelmässige Bewertungen durchzuführen, um sicherzustellen, dass die als Reaktion auf Cybersicherheitsvorfälle ergriffenen Massnahmen tatsächlich effektiv sind.

TRY AND ERROR - KONTINUIERLICH AUS FEHLERN LERNEN

Ein kontinuierlicher Lern- und Verbesserungsansatz ist entscheidend für die Steigerung der Cyber-Resilienz in Organisationen.



LEITLINIEN FÜR SCHWEIZER UNTERNEHMEN BASIEREND AUF DER STUDIE AUS DEM VEREINIGTEN KÖNIGREICH

Basierend auf der Studie „*I don't think we're there yet: The practices and challenges of organisational learning from cyber security incidents*", können Schweizer Unternehmen mehrere Massnahmen ergreifen, um ihre Cybersicherheit zu verbessern. Es empfiehlt sich,

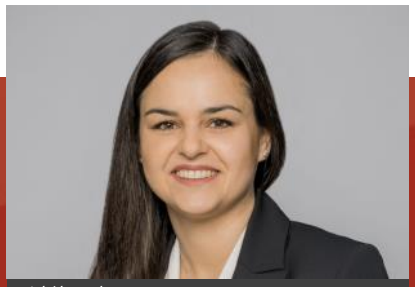
regelmässig die eigenen Lernpraktiken aus Cybersicherheitsvorfällen zu bewerten und eine Kultur der Offenheit zu fördern, in der das Melden von Cybersicherheitsvorfällen und das Lernen aus Fehlern ermutigt wird. Eine einheitliche Methode zur Klassifizierung dieser Vorfälle ist für die Standardisierung der Reaktion wichtig. Ebenso ist eine tiefergehende Analyse der Ursachen unerlässlich, um systemische Faktoren zu erkennen und effektive Gegenmassnahmen zu entwickeln. Weiter sollten die gewonnenen Erkenntnisse nicht nur identifiziert, sondern auch effektiv umgesetzt und kontinuierlich überwacht werden. Eine transparente Kommunikation mit Lieferanten und Partnern sowie die Förderung von Weiterbildung und Fachwissen im Bereich Cybersicherheit sind ebenfalls zentrale Aspekte. Abschliessend sollten Unternehmen den Austausch von Informationen und die Zusammenarbeit innerhalb der Branche und mit Regulierungsbehörden fördern, um gemeinsam aus Vorfällen zu lernen und sich an neue Bedrohungen anzupassen.

ZUSAMMENFASSUNG

Die Studie *„I don't think we're there yet: The practices and challenges of organisational learning from cyber security incidents"* unterstreicht die Wichtigkeit eines kontinuierlichen und organisationalen Lernprozesses zur Stärkung der Cyber-Resilienz. Obwohl sie auf Daten aus dem Vereinigten Königreich basiert, können die Erkenntnisse auch für Schweizer Unternehmen von Bedeutung sein. Unternehmen sind gefordert Cybersicherheitsvorfälle nicht nur als Risiko, sondern als Chance zum Lernen und zur Stärkung ihrer Abwehrkräfte zu begreifen. Dies erfordert eine regelmässige Überprüfung und Anpassung der Lernpraktiken sowie die Etablierung einer offenen und transparenten Unternehmenskultur. In dieser Kultur sollte das Melden von Cybersicherheitsvorfällen sowie das Lernen aus Fehlern aktiv gefördert werden. Zudem wird die Bedeutung der Anpassung an sich ständig entwickelnde Cyberbedrohungen betont. Die fortschreitende Integration neuer Technologien und die zunehmende globale Vernetzung führen zu einer Erhöhung der Cybersicherheitsrisiken. In diesem Kontext ist es für Unternehmen unerlässlich, ihre Sicherheitsfähigkeiten fortlaufend zu verbes-

sern und sich flexibel an die dynamischen Bedrohungslagen anzupassen. Ein weiterer Punkt ist die gründliche Analyse von Sicherheitsvorfällen. Nur durch eine detaillierte Untersuchung der Ursachen können systemische Schwachstellen identifiziert und effektive Gegenmassnahmen entwickelt werden. Die aus solchen Analysen gewonnenen Erkenntnisse sollten nicht nur identifiziert, sondern auch konsequent umgesetzt und regelmässig überprüft werden, um ihre Wirksamkeit sicherzustellen. Die Studie hebt auch die Bedeutung von Kommunikation und Zusammenarbeit hervor.

Eine offene und transparente Kommunikation mit Lieferanten, Partnern und innerhalb der Branche ist essenziell, um aus Vorfällen kollektiv zu lernen und sich gemeinsam an neue Bedrohungen anzupassen. Der Austausch von Informationen und die Kooperation mit Regulierungsbehörden sind ebenfalls wichtige Aspekte, um effektiv auf Cybersicherheitsvorfälle reagieren zu können. Zudem ist es angesichts des Mangels an qualifizierten Cybersicherheitsexperten für Unternehmen unabdingbar, in die Aus- und Weiterbildung ihrer Mitarbeiter zu investieren und Fachwissen im Bereich Cybersicherheit zu fördern. Dies trägt massgeblich dazu bei, die Fähigkeiten und Kompetenzen im Umgang mit Cyberrisiken zu stärken.



Michèle Trebo

Threat Intelligence 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 und Threat Intelligence so einfach. Setzen Sie sich mit uns in Verbindung!

https://vuldb.com

Bilderquelle: https://unsplash.com/photos/green-trees-under-white-clouds-Zm9KsuOiJDU

MICHAEL SCHNEIDER

BERICHT UND DOKUMENTATION: UNBELIEBT UND DOCH SO WICHTIG

Das Erstellen von Dokumentationen oder das Verfassen von Berichten ist für die meisten Techniker keine beliebte Aufgabe. Die IT-Sicherheit bildet hier keine Ausnahme. Neben technischem Wissen sollten Penetration Tester auch die Fähigkeit haben, Berichte zu schreiben und klar zu kommunizieren, auch mit Personen, die keine vertieften technische Kenntnisse haben. Der Bericht zeigt dem Kunden, was in einem Test geprüft und festgestellt wurde. Die meisten Kunden bekommen nicht mit, was während eines Tests passiert, daher gilt: Was nicht im Bericht steht, ist auch nicht passiert.

Nicht weniger wichtig ist die Dokumentation von Techniken, Werkzeuge, Erfahrungen und Wissen. Neu gelernte Techniken und gemachte Erfahrungen sollten so festgehalten werden, dass sie auch in der Zukunft nützlich sind, mit anderen geteilt werden können oder erstmals überhaupt nach einem halben Jahr wieder gefunden werden. Manchmal weiss man noch, dass man etwas schon einmal aufgeschrieben hatte, findet aber keine Aufzeichnungen mehr darüber.

BERICHT

Nach dem Abschluss einer Sicherheitsprüfung erhält der Kunde einen Bericht. Der Bericht soll Schwachstellen aufzeigen und Empfehlungen zu deren Behebung geben. Es wird festgehalten, was der Scope der Prüfung war, welche Bereiche getestet wurden und wie der Test ausgefallen ist. Schwachstellen sollen so dokumentiert sein, dass sie durch den Kunden nachvollziehbar sind.

Unsere Berichte sind nach dieser Struktur aufgebaut:

- Summary: Management Summary, Resultatgrafiken, Fragen und Antworten
- Administration: Änderungsprotokoll, Verteilerliste, Projektteam
- Einleitung: Beschreibung und Ziele des Projekts, Scope-Definition
- Resultate: Modalitäten, Auflistung Resultate mit Gegenmassnahmen

- Appendix: Liste der eingesetzten Tools, Definierung Schweregrad, Indexierungslisten

Auf die Inhalte Management Summary und Resultate wird weiter im Text eingegangen. Im Kapitel Einleitung des Berichts werden Auftrag und der Scope festgelegt. Es wird beschrieben, welchen Umfang die Sicherheitsprüfung und der Bericht haben und ob bestimmte Bereiche nicht geprüft wurden. Die Modalitäten enthalten technische Informationen, welche Benutzerkonten mit welchen Berechtigungen, welche Systeme und IP-Adressen verwendet wurden und von wann bis wann die Prüfung dauerte. Ebenso wird eine Liste der für die Überprüfung erhaltenen Dokumente erstellt. Es wird dokumentiert, ob Sicherheitskontrollen wie eine Web Application Firewall (WAF) deaktiviert wurden und ob während der Prüfung Änderungen wie die Installation von Updates vorgenommen wurden.

MANAGEMENT SUMMARY

Das Management Summary wird adressatengerecht verfasst. Die Formulierungen sollten klar und einfach verständlich sein. Technische Details gehören in der Regel nicht in ein Management Summary, es sei denn, es handelt sich explizit um einen technischen Leserkreis. Dies kann schwierig sein, da der innere Drang unterdrückt werden muss, die Ausnutzung einer komplexen Schwachstellen in allen Einzelheiten zu demonstrieren. Die Ausnutzung der Schwachstelle kann jedoch im Kapitel Resultate ausführlich beschrieben werden.

Die Erfahrung beim Schreiben von Berichten lehrt, dass das Management Summary nicht allen gefallen wird. Insbesondere Ergebnisse mit kritischen Schwachstellen können zu Diskussionen und Kontroversen führen. Deshalb sollte das Summary faktenbasiert geschrieben sein und auf Politik oder gar Polemik verzichtet werden. Die Ergebnisse müssen nachvollziehbar dokumentiert und die Bewertungen messbar sein, da sie als Grundlage für die Aussagen im Summary dienen.

Zu jeder Bewertung in einem Management Summary respektive im gesamten Dokument gehört eine Metrik. Es muss klar sein, wie eine Bewertung zustande kommt oder wie eine Aussage zu messen ist. Der Satz “Das Resultat ist genügend”, ohne zu defi-

nieren, was genügend ist, lässt Interpretationsspielraum und macht es dem Leser unmöglich, das Resultat einzuordnen. Auch die Frage, wie viele der Findings behoben werden müssen, damit das Resultat als gut eingestuft wird, kann so nicht fundiert beantwortet werden. Im Artikel zum HardeningKitty Score habe wir uns mit dem Sinn und Unsinn einer solchen Bewertung für ein komplexes Konstrukt auseinandergesetzt. Wir verzichten daher auf so eine einfache Bewertung und listen stattdessen im Management Summary in einem Absatz kritische und wichtigsten Schwachstellen, die Statistik der gefundenen Schwachstellen sowie in weiteren Abschnitten die Stärken und Schwächen des Prüfobjekts auf.

RESULTATE

Veit Hailperin hatte sich bereits 2016 im Artikel Checklisten oder Szenarien mit der idealen Art der Dokumentation einer Sicherheitsprüfung beschäftigt. Wir verwenden nach wie vor Checklisten für Konzept-, Konfigurations- und Systemreviews sowie für Penetration Tests von Web- oder Mobile-Applikationen. Bei Assessments, wie der Simulation bestimmter Angriffstechniken oder einem Red Team Assessment, setzten wir auf eine Mischung aus szenario- und checklistenbasierten Dokumentation.

Wir dokumentieren alle Tests in Checklisten, um transparent zu machen, was alles geprüft wurde und um die Vollständigkeit zu gewährleisten. Der Kunde erfährt nicht nur, wo die Schwachstellen seines Zielobjekts liegen, sondern auch, welche Bereiche bereits gesichert sind. Wird eine Schwachstelle gefunden, dokumentieren wir diese so, dass der Kunde sie bei Bedarf selbst reproduzieren kann. Hier können technische Details dargestellt und gezeigt werden, wie eine Schwachstelle ausgenutzt werden konnte. Der innere Drang, den Proof of Concept (PoC) in allen Details nachzuweisen, kann und soll hier ausgelebt werden. Dazu gehört neben der technischen Beschreibung einer Schwachstelle auch die Beweisführung, beispielsweise durch das Hinzufügen von Requests und Responses im Falle einer Web-Schwachstelle. Für jede Schwachstelle wird ein Schweregrad festgelegt. Wir verwenden die Einstufungen Passed, Low, Medium, High und Emergency, welche am Industriestandard CVSS v3.1 angelehnt sind. Zusätzlich wird für jede Schwachstelle auch eine Gegenmassnahme vorgeschlagen.

Neben dem Report als PDF geben wir die Resultate in einem maschinenlesbaren Format ab, entweder in unserem eigenen oder in einem vom Kunden definierten Format. Dies soll die Weiterverarbeitung der Resultate erleichtern, so dass diese in ein Risk-Management- oder Ticket-System importiert werden können, ohne dass ein Kopieren und Einfügen aus einem PDF erforderlich ist.

DOKUMENTATION VON WISSEN

Neben dem Verfassen eines Berichts ist das Dokumentieren von Wissen eine weitere wichtige Tätigkeit, welche die Fähigkeiten im Schreiben von Texten erfordert. Auch wenn das Wissen nur für sich selbst festgehalten wird. Was zum Zeitpunkt der Anwendung völlig klar erscheint, bedarf zu einem späteren Zeitpunkt, wenn man sich schon länger nicht mehr mit dem Thema beschäftigt hat, einer zusätzliche Erklärung. Deshalb sind Notizen so wichtig und kleinere Details können den Unterschied zwischen Erfolg und Misserfolg ausmachen. Wenn beispielsweise bei einem Tool ein bestimmter Parameter notwendig ist, damit der Angriff erfolgreich ist, dieser Parameter aber nur beiläufig im Aufruf steht, ohne dass darauf hingewiesen wird, dass er korrekt gesetzt werden muss, kann dies leicht untergehen. Insbesondere dann, wenn die eigenen Notizen nun doch mit jemand anderem geteilt werden und diese Person sich der Bedeutung nicht bewusst ist. Die Projekte The Hacker Recipes von Charlie Bromberg sowie PayloadsAllTheThings und Internal All The Things von Swissky sind vorbildlich und eine tolle Wissensquelle.

Der Informationsfluss im Bereich der IT-Security ist enorm und Veränderungen treten häufig auf. Neue Tools und Angriffstechniken werden veröffentlich, bestehende Techniken werden detektiert und müssen angepasst werden oder es werden neue Schwachstellen entdeckt, die bisher ungeahnte Möglichkeiten bieten. Wissen wird nicht nur durch neue Informationen erworben, sondern auch durch eigene Recherchen, Training, Teilnahme an Weiterbildungen und Konferenzen oder auch durch den Austausch mit Gleichgesinnten. Um all dieses Wissen festhalten zu können, braucht es Schreibfähigkeiten, Disziplin, aber auch die richtigen Werkzeuge.

WERKZEUGE

Im Laufe der Zeit habe ich verschiedene Tools ausprobiert. Zu Beginn war das ungeordnete Sammeln von Bookmarks, Textdateien und PDFs, darauf folgte Notepad++ mit Plugins und Tools wie Microsofts OneNote oder später die Open-Source-Alternative CherryTree. Während OneNote ein proprietäres Format zum Speichern der Notizbücher verwendet, unterstützt CherryTree SQLite oder XML-Dateien. Ich wollte weg von Tools, die alles in eine Datei packen, und habe Markdown mit Sublime und ReStructured-Text mit Sphinx ausprobiert und je nach Projekt immer noch im Einsatz. Aktuell verwende ich Obsidian und bin daran meine bestehenden Sammlungen zu konvertieren.

Obsidian arbeitet mit dem Markdown-Format, ermöglich das Erstellen von Strukturen und unterstützt das Verbinden von Notizen mit Links, stellt Verknüpfungen in Graphen dar und bietet die Möglichkeit einfache Diagramme oder Workflows zu zeichnen. Zudem kann mit Templates vieles automatisiert und vorgegeben werden. Sam Link von TrustedSec zeigt im Artikel Obsidian, Taming a Collective Consciousness wie dies genutzt werden kann.

ANWENDUNG

Werkzeuge allein nützen nichts, sie müssen auch eingesetzt werden. Meine Vorgehen ist so, dass ich eine Liste mit offenen Aufgaben führe, neue Informationen wie zum Beispiel ein Tool landen in dieser Liste. Nach der Abarbeitung eines Punktes der Liste und der Informationsverarbeitung dokumentiere ich dies entsprechend. Meistens geschieht dies in meinem persönlichen Obsidian Vault. Die Dokumentation ist zunächst knapp gehalten, beispielsweise eine

Liste von Befehlen, wie etwas angewendet respektive umgesetzt wird. Mit Obsidian kann ich diese neue Information mit bestehendem Wissen verknüpfen, beispielsweise wenn ich eine neue Angriffstechnik dokumentiere, kann ich diese in die bestehende Struktur einbetten und Links zu ähnlichen Techniken oder der Grundlagendokumentationen setzen. Als nächstes versuche ich die Befehle zu verallgemeinern, unter anderem durch Verwendung von Variablen anstelle festen Werten. Ausserdem beschreibe ich, was mit dem Befehl bezweckt wird und erwähne, warum ein bestimmter Parameter so gesetzt werden muss oder was sonst noch zu beachten ist. Je nach Thema gebe ich die Informationen weiter, indem ich sie in eine bestehende Sammlung einfüge oder anderweitig veröffentliche.

Natürlich ist manchmal das Verlangen, das neues Wissen auszuprobieren und weiter zu experimentieren, grösser ist als die Motivation, das erarbeitete Wissen noch sauber aufzuschreiben, oder die Dokumentation bleibt dann erstmals halbfertig. Aus der Erfahrung heraus, dass mich die unfertige Dokumentation früher oder später einholen wird, stelle ich mir dann eine Aufgabe mit Erinnerung, die Dokumentation später fertig zu stellen. Für mich funktioniert das gut, andere haben andere Tricks und Angewohnheiten um dies zu lösen. Wichtig ist, dass es gelingt, das Gelernte vollständig zu dokumentieren.

FAZIT UND AUSBLICK

Das Verfassen von Berichten und Dokumentationen ist nicht jedermanns Sache. In unserer Arbeit ist es jedoch unerlässlich und es sollte entsprechend geübt werden. Übung, Erfahrung und Diskussionen mit Kunden und Kollegen verbessern die eigenen Fähigkeiten, einen guten Bericht zu verfassen. Spätestens

wenn man einen Retest mit einem Bericht durchführen muss, den man nicht selbst geschrieben hat, schätzt man eine ausführliche, klare Beschreibung mit technischen Details und reproduzierbaren Beispielen.

Das Dokumentieren von Wissen mag auf den ersten Blick keine glamouröse Tätigkeit sein, aber ohne Dokumentation ist es schwieriger, Wissen zu teilen. Es ist auch schwierig, eine komplexe Angriffstechnik zu reproduzieren, wenn keine Notizen über den Aufbau und die Anwendung vorhanden sind. Zudem wenn etwas vollständig niedergeschrieben ist, bleibt es auch länger erhalten. Ein passendes Werkzeug vereinfacht die Dokumentation. Wir sind dankbar für all die Arbeit, die in die Dokumentation von Protokollen, Angriffstechniken, Tools und vielem mehr gesteckt wird. Das macht es uns leichter neues Wissen zu erwerben. Deshalb leisten wir unseren Beitrag, indem wir Dokumentationen erstellen und teilen.

Es gibt noch einen Elefant im Raum und zwar die Nutzung von Large Language Models (LLM) zur Erstellung von Berichten. Eine Liste von Findings wird einem LLM zur Verfügung gestellt und heraus kommt ein Bericht inklusive Management Summary. Das ein Wunschtraum, der auch in einigen Jahren noch nicht Realität sein wird. LLM-Tools können unterstützend für die Generierung der Beschreibung einzelner Findings oder Gegenmassnahme, zur Übersetzung von Texten oder zur Verbesserung des Stils eingesetzt werden. Das ein LLM ein akkurates Management Summary verfassen wird oder gar einen vollständigen Bericht erstellen kann, daran glaube ich im Moment nicht (Januar 2024). Ich lasse mich gerne eines Besseren belehren.


Michael Schneider

AUF DER PISTE WIE AUCH IN DER DIGITALEN WELT GILT SAFETY FIRST.

Bildquelle: https://unsplash.com/de/fotos/graustufenfoto-von-seilbahnen-AePWt_L3XAI

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