MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE JUNI 2022
DATENHEHLEREI UND VERTRAUEN IN MASCHINEN

HANDEL MIT GESTOHLENEN DATEN

Wir zeigen die Funktionsweise, die rechtlichen Grundlagen und Möglichkeiten einer Verhandlungsführung beim Umgang mit gestohlenen Daten.

VERWUNDBARKEIT VON MENSCH UND MASCHINE

Vertrauen geht immer mit einer gewissen Verwundbarkeit einher. Dass die Vertrauensbeziehung zu Maschinen noch nicht genügend erforscht ist, zeigt unser Beitrag.

Juni 2022: Unsichere App Stores

Modularität ist ein wichtiges Konzept der modernen IT-Landschaft. Viele Produkte bieten mittlerweile das Nachrüsten von Funktionalität mittels Plugins, Addons, Extensions und Apps an. Einer der wichtiger Vorreiter, der dieses Prinzip breitflächig bekannt gemacht hat, ist der populäre Webbrowser Firefox. Mit dem Installieren von Add-Ons wird es gar möglich, den Browser um komplexe Mechanismen zu erweitern.

In anderen Bereichen hat dieses Konzept ebenso Früchte getragen und massgeblich zum Erfolg ganzer Industriezweige beigetragen. Zum Beispiel die beim Apple iPhone nutzbaren Apps, die zusätzliche Software auf dem Gerät installieren lassen. Oder die bei Facebook aktivierbaren Third-Party Applications, durch die Auswertungen, Informations-Austausch und Spiele möglich werden.

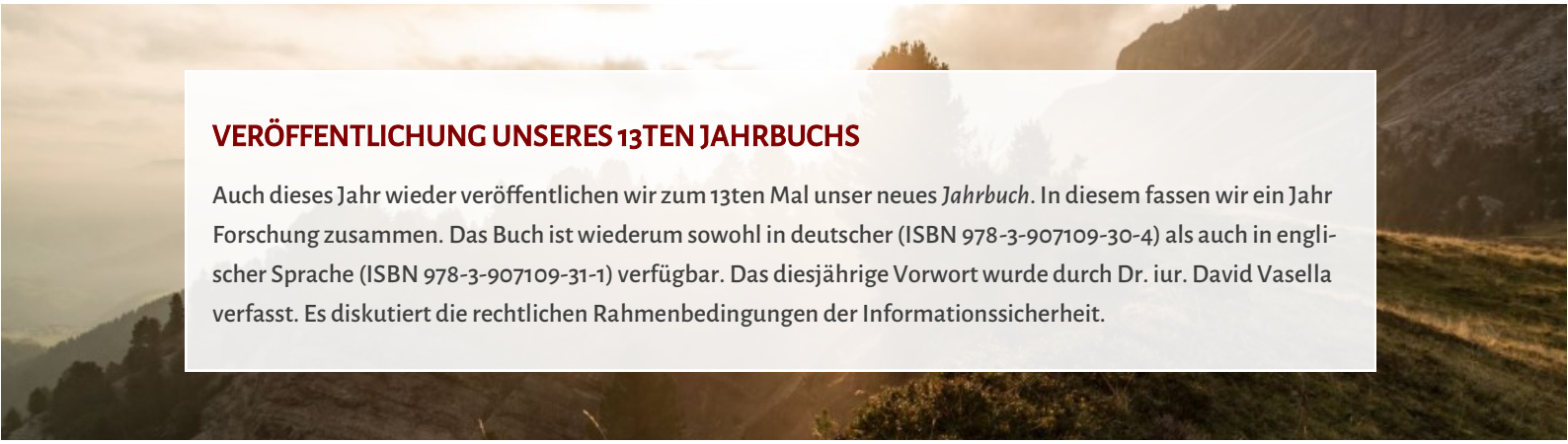
Doch ein Angreifer kann die bereitgestellten Mechanismen missbrauchen, um eine böswillige Komponente erstellen und verbreiten zu lassen. Attacken auf Nutzer und Missbrauch der bereitgestellten Zugriffsmöglichkeiten könnten die Folge davon sein.

Apple sieht zum Beispiel in ihrem Prozess vor, dass eine für den Store vorgesehene App zuerst reviewed werden muss. Erst nach einer Prüfung wird die Freigabe erteilt. Dadurch kann sowohl die Qualität als auch die Sicherheit der App gewährleistet werden. Doch das Problem ist, dass eine Prüfung mit sehr viel Aufwand verbunden und fehleranfällig ist. Ab und an schafft es halt doch eine böswillige App in einen Store.

Marc Ruef
Head of Research

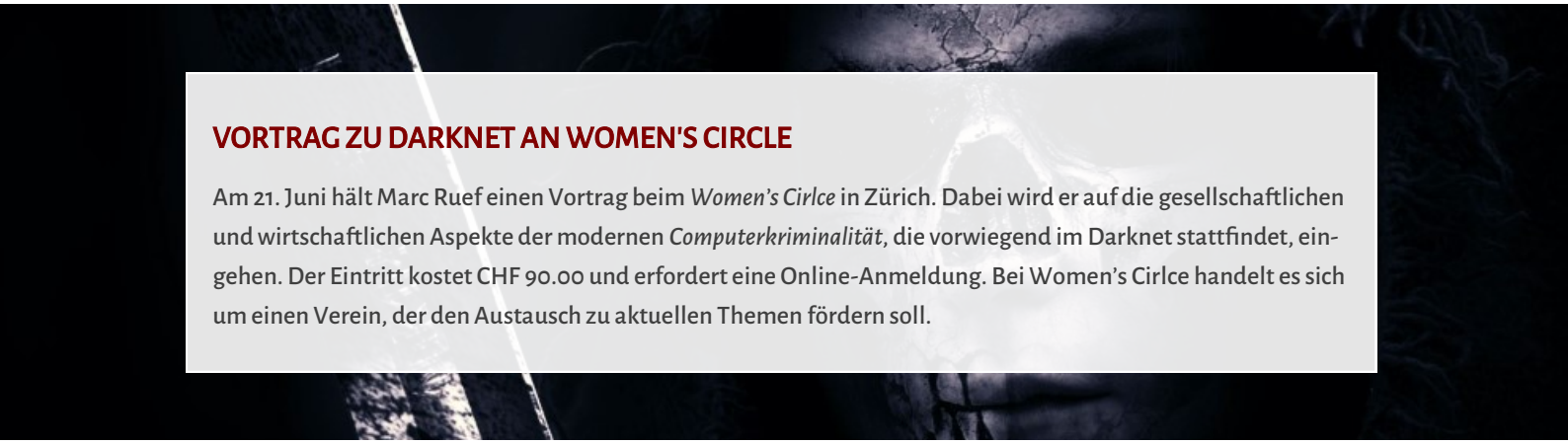
NEWS

WAS IST BEI UNS PASSIERT?



VERÖFFENTLICHUNG UNSERES 13TEN JAHRBUCHS

Auch dieses Jahr wieder veröffentlichen wir zum 13ten Mal unser neues *Jahrbuch*. In diesem fassen wir ein Jahr Forschung 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 diesjährige Vorwort wurde durch Dr. iur. David Vasella verfasst. Es diskutiert die rechtlichen Rahmenbedingungen der Informationssicherheit.



VORTRAG ZU DARKNET AN WOMEN'S CIRCLE

Am 21. Juni hält Marc Ruef einen Vortrag beim *Women's Cirlce* in Zürich. Dabei wird er auf die gesellschaftlichen und wirtschaftlichen Aspekte der modernen *Computerkriminalität*, die vorwiegend im Darknet stattfindet, eingehen. Der Eintritt kostet CHF 90.00 und erfordert eine Online-Anmeldung. Bei Women's Cirlce handelt es sich um einen Verein, der den Austausch zu aktuellen Themen fördern soll.

VERÖFFENTLICHUNG VON SCHWACHSTELLE IN FILECLOUD

Andrea Hauser und Ralph Meier haben eine Schwachstelle im Produkt *FileCloud* gefunden. Diese wurde im Rahmen unseres *Responsible Disclosure Prozesses* in Zusammenarbeit mit dem Hersteller adressiert und publik gemacht. Das Vendor-Advisory ist ebenso verfügbar wie ein offizieller CVE-Eintrag als CVE-2022-1958. Der Fehler wurde in Version 21.3.5.18513 behoben.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

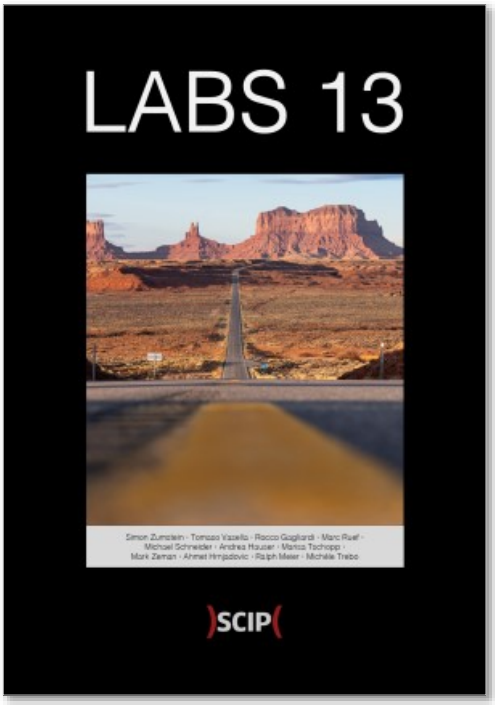
UNSER NEUES JAHRBUCH

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.



ISBN 978-3-907109-30-4 [de]
ISBN 978-3-907109-31-1 [en]

MANCHES GESCHIEHT NUR IM UNTERGRUND

Bildquelle: https://pixabay.com/images/id-21668/

MICHÈLE TREBO

DATENHEHLEREI ALS VERBOTENER UMGANG MIT GESTOHLENEN DATEN

Datenhehlerei ist ein Begriff der so im Schweizerischen *Strafgesetzbuch StGB* nicht explizit existiert, aber dennoch strafbar ist. Die Hehlerei nach Art. 160 StGB sagt aus, dass eine Sache – in diesem Fall Daten -, von denen man weiss oder annehmen muss, dass sie ein anderer durch strafbare Handlungen gegen das Vermögen erlangt hat, erwirbt, sich schenken lässt, zum Pfande nimmt, verheimlicht oder veräussern hilft, mit einer Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft wird. Handelt die Täterschaft gewerbsmässig, so wird sie mit einer Freiheitsstrafe von bis zu zehn Jahren oder einer Geldstrafe nicht unter 90 Tagessätzen bestraft. Doch was bedeutet das genau?

Bevor es überhaupt zur Datenhehlerei kommen kann, müssen die *Daten* vorgängig durch eine *strafbare Handlung gegen das Vermögen* erlangt worden sein. Dabei wird oft unbefugt in ein Datenverarbeitungssystem eingedrungen, sowie das Art. 143 bis 182 StGB unter Strafe stellt. Dabei dringt beispielsweise eine unbekannte Täterschaft, wir nennen sie die *Panzerknacker*, in das Datenverarbeitungssystem der *Firma Duck* ein und entwendet sensible Kundendaten. Nicht nur das unbefugte Eindringen in das Datenverarbeitungssystem, sondern auch das Entwenden der Daten (Diebstahls nach Art. 139 StGB) erfüllen bereits Straftatbestände.

Nun sind die Panzerknacker in Besitz der Kundendaten der Firma Duck und möchten damit Geld verdienen. Sie können dies auf *zwei Arten* tun. Entweder sie *erpressen* die Firma Duck (Erpressung nach Art. 156 StGB), indem sie mit ihr Kontakt aufnehmen und für das Zurückgeben/Löschen der Daten einen bestimmten Geldbetrag verlangen oder sie bieten die Kundendaten im Web *zum Verkauf* an. Die Hehler, in diesem Fall die Panzerknacker, werden nach der Strafandrohung der Vortat bestraft, wenn diese milder ist. Ist die Vortat ein Antragsdelikt, so wird die Hehlerei nur verfolgt, wenn ein Antrag auf Strafverfolgung der Vortat vorliegt (Hehlerei nach Art. 160 StGB). Im Fallbeispiel entscheiden sich die Panzerknacker, die gestohlenen Kundendaten der Firma Duck auf einem Online-Marktplatz für geleakte Daten zum Verkauf anzubieten. Donald entdeckt das Angebot der Panzerknacker und möchte ebenfalls von diesen Daten profitieren. Er überweist den Panzerknackern Kryptowährung und erhält dafür die geleakten Daten der Firma Duck. Bereits durch den Kauf dieser Daten hat sich Donald der Hehlerei nach

Art. 160 StGB strafbar gemacht. Würde er die Daten verkaufen, wäre auch das strafbar.

DATENHEHLEREI VS. RANSOMWARE

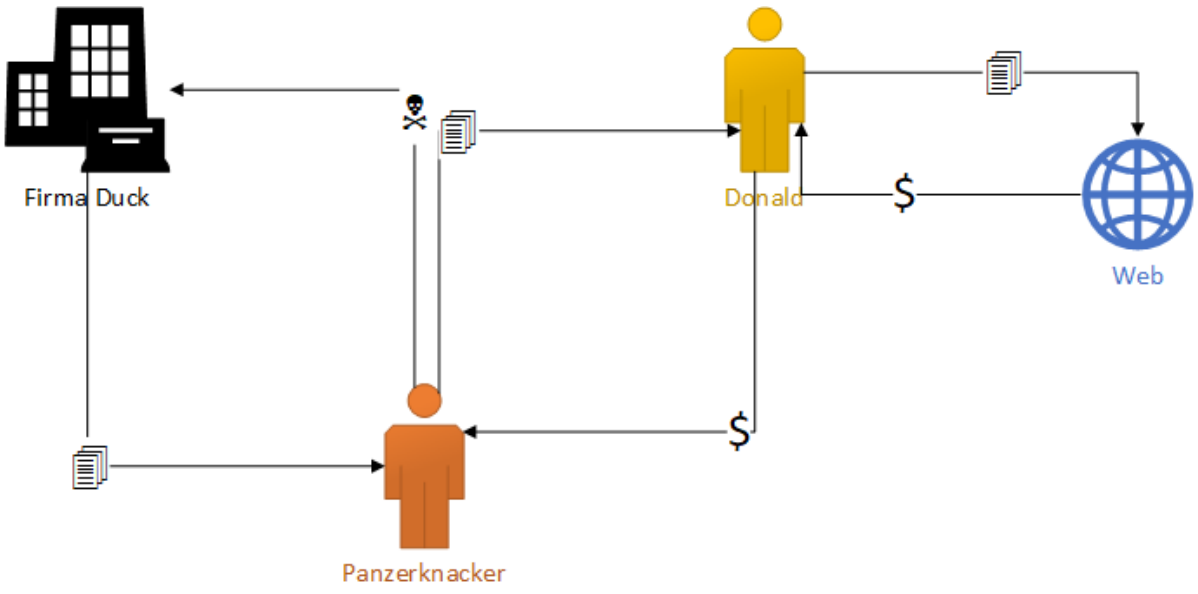
Die Datenhehlerei ist nicht mit *Ransomware* zu verwechseln. Bei Ransomware erpresst die Täterschaft Lösegeld für das Freigeben eines Computers oder der Daten, die sich darauf befinden. Dabei nutzt die Täterschaft im Gegensatz zur Datenhehlerei *Schadprogramme*, mit deren Hilfe sie den Zugriff auf Daten, deren Nutzung oder das ganze Computersystem verhindern kann.

SCHUTZ VOR CYBERANGRIFFEN

Egal ob als Privatperson oder Unternehmen, sich über Cyberangriffe zu informieren und sich entsprechend davor zu schützen, ist in der heutigen Zeit nicht mehr wegzudenken. Wer nicht zum Opfer werden will, sollte regelmässig den Ernstfall prüfen, um Schwachstellen zu detektieren und frühzeitig beheben zu können.

Private

Privaten wird empfohlen, den Webbrowser, das Betriebssystem und Software aktuell zu halten. Ausserdem erschwert ein Virenschutz und eine Firewall einem möglichen Angreifer das Eindringen. Allgemein sollte darauf geachtet werden, ein sicheres und für jedes Log-in ein separates Passwort zu wählen. Dabei kann ein Passwortmanager unterstützen. Passwörter sollten mindestens zehn Zeichen lang sein, Gross- und Kleinschreibung, Zahlen und Sonderzeichen enthalten. Zudem wird davon abgeraten, Passwörter zu wählen, die mit dem Benutzter in Verbindung stehen oder tatsächliche Wörter enthalten.



Weiter kann die Sicherheit bez. Log-in verbessert werden, indem man sich wo möglich für eine Zwei-Faktor-Authentisierung entscheidet. Bevor eine Email oder dessen Anhang geöffnet wird, ist es wichtig, sich zu überlegen, was dahinterstecken könnte. Auch Downloads sollten wohl überlegt sein. Zusätzlich sollte darauf geachtet werden, stets eine verschlüsselte Internetverbindung zu verwenden (HTTPS).

Unternehmen

Unternehmen wird empfohlen, das Sicherheitsmodell in regelmässigen Abständen zu überprüfen oder überprüfen zu lassen. Dabei können Security-Assessments, Penetration-Tests usw. Aufschluss über mögliche Schwachstellen geben. Wichtig ist es auch, Mitarbeiter auf mögliche Cyberangriffe zu sensibilisieren und den Umgang mit der Infrastruktur zu schulen. Ein Notfallkonzept für den Ernstfall kann helfen, zeitnah richtig reagieren zu können. Weiter sind externe Daten-Back-ups sowie ein sicherer Datenaustausch Möglichkeiten, Cyberangriffen entgegenzuwirken.

VERHALTEN IM ERNSTFALL

Wie verhalten Sie sich, wenn Sie trotz aller Vorsichtsmassnahmen Opfer von Datenhehlerei werden? Zuerst ist zu prüfen, wie hoch die Wahrscheinlichkeit ist, dass die Täterschaft tatsächlich in Besitz Ihrer Daten ist. Möglicherweise möchte sie nur an Geld kommen und die tatsächlichen Daten liegen gar nicht vor. Dabei kann beispielsweise bei der Täterschaft nach einem Beispieldatensatz gefragt werden. Sollte die Möglichkeit bestehen, dass die Täterschaft die echten Daten hat, so sollten entsprechende Massnahmen eingeleiten werden. Vom Begleichen des geforderten Geldbetrages wird abgeraten. Denn ob die Täterschaft die geleakten Daten anschliessend nicht weiterverkauft oder löscht, ist nicht garantiert. In diesem Fall wird empfohlen, sich an Spezialisten zu wenden.

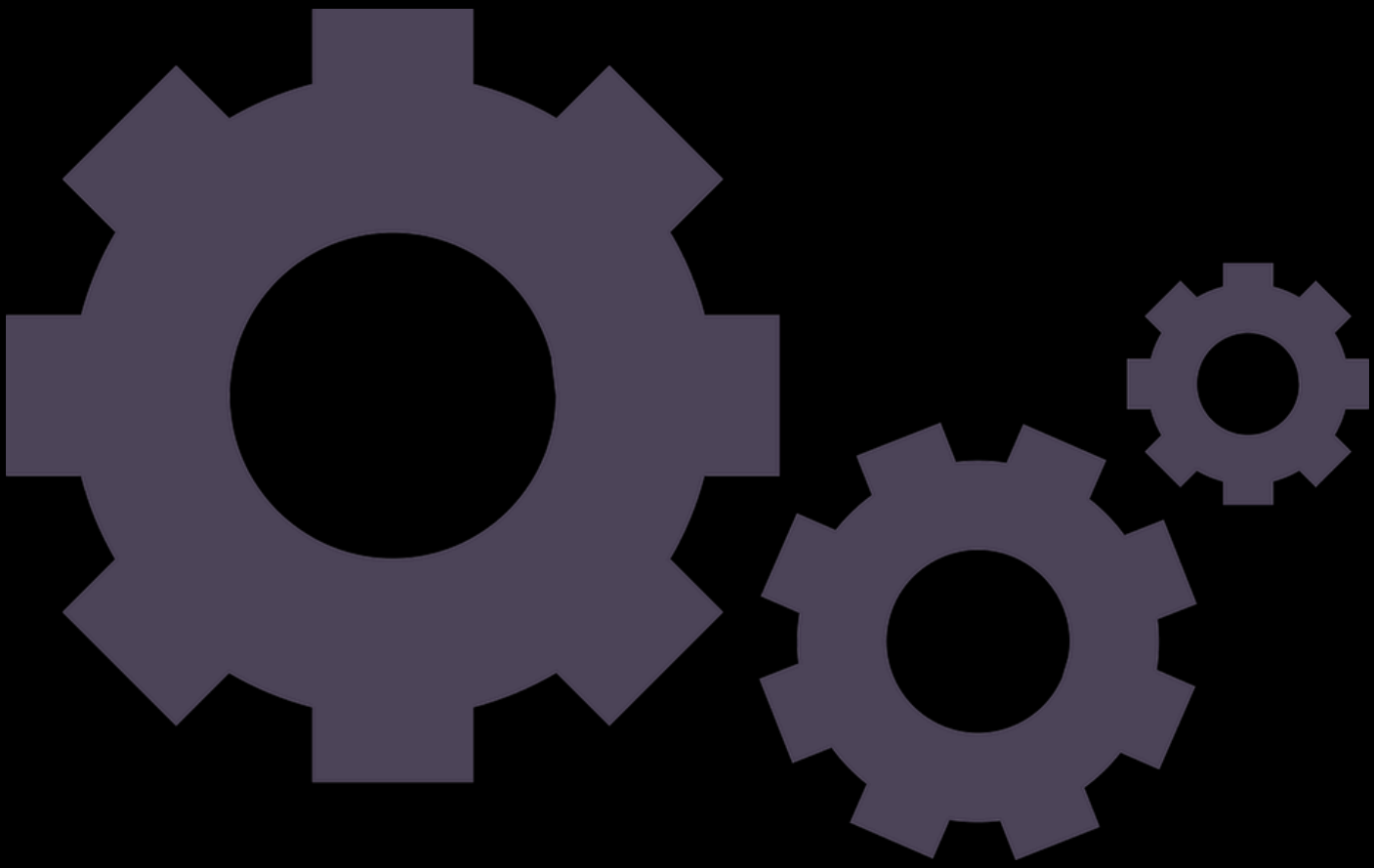
ZUSAMMENFASSUNG

Cyberangriffe sind mittlerweile Alltag und sollten nicht ausser Acht gelassen werden. Mit einfachen Tricks kann man solchen vorbeugen und nicht nur sich, sondern auch das Unternehmen schützen. Besonders im Ernstfall wie der Datenhehlerei sollte man richtig reagieren und gewappnet sein. Die Datenhehlerei existiert nicht explizit im Schweizerischen Strafgesetzbuch StGB. Dennoch ist sie strafbar und es können mehrere Straftatbestände erfüllt sein. Dabei können beispielsweise der Diebstahl nach Art. 139 StGB, das unbefugte Eindringen in ein Datenverarbeitungssystem nach Art. 143 bis 182 StGB, die Erpressung nach Art. 156 StGB sowie die Hehlerei nach Art. 160 StGB zur Anwendung kommen. Sollten Sie sich nicht sicher sein, ob Sie genügend geschützt sind oder Opfer eines Cyberangriffes geworden sein, unterstützen wir Sie gerne.

Michèle Trebo

next gen vulnerability intelligence

VulDB



Werden Sie Teil der Community

Durch die tägliche Dokumentation neuer Schwachstellen, detaillierte Analyse der technischen Hintergründe, exklusive Details zu Exploiting und Gegenmassnahmen erhalten Sie mit vuldb.com ein durchschlagskräftiges Werkzeug in die Hand. Das Projekt wird durch eine aktive Community unterstützt, die neue Schwachstellen dokumentiert und bestehende Einträge aktualisiert. Seien Sie einen Schritt voraus!

)SCIP(
official data provider

https://vuldb.com

MARISA TSCHOPP

VERWUNDBARKEIT VON MENSCH UND MASCHINE

Wie stark wir Systemen mit *künstlicher Intelligenz* (KI) vertrauen, beeinflusst, ob wir uns auf diese verlassen und wie wir sie nutzen. Die *Einflussfaktoren* auf das Vertrauen zu erforschen, stösst auf grosses Interesse, während Verletzlichkeit in der Mensch-Maschine-Interaktion nicht wirklich viel Beachtung findet. Dabei ist Verletzlichkeit das Herzstück der Vertrauenstheorien in menschlichen Interaktionen. Trotzdem ist Verletzlichkeit nicht das Herzstück der Vertrauenstheorien in der Mensch-Maschine-Interaktion. Noch nicht. Was ist Verletzlichkeit? Bei Menschen bedeutet Verletzlichkeit, dass sie in einer Interaktion ein gewisses Risiko eingehen, vom Gegenüber enttäuscht zu werden: Sie machen sich verletzlich gegenüber anderen. Erst Vertrauen macht es Menschen möglich, trotz schlechter Vorhersagbarkeit und Unsicherheit den sogenannten Glaubenssprung (Leap of Faith) in unbekannte Gewässer mit unbekannten Menschen zu wagen.

Derzeit wird viel über *vertrauenswürdige KI* diskutiert. Diese hat zum Ziel, das Risiko für Menschen verletzt zu werden, zu reduzieren. Um vertrauenswürdige KI zu erreichen, werden Ideale aufgestellt, wie ein KI-System auszusehen hat. KI muss unter anderem technisch robust und sicher sein, die Modelle müssen transparent, erklärbar oder auditierbar sein. Diese Leitlinien sind deshalb sinnvoll, weil KI-Systeme *Schwachstellen* haben. Sie funktionieren nie perfekt, was ein KI-System ebenfalls verletzbar macht. Wobei in der IT der Begriff verwundbar besser passt und vor allem in der IT-Security bereits einen festen Platz hat.

ÜBERALL SIND SCHWACHSTELLEN

Diese Schwachstellen (oder Verwundbarkeiten) sind eine von vielen Ursachen, warum es bei KI-Systemen zu einer Situation geprägt von *Unsicherheit* kommt. Das ist auch der Grund, warum es überhaupt zu einer Vertrauensbeziehung zwischen Mensch und Maschine kommt. Die Krux ist jedoch, dass am Ende nur Menschen wirklich verletzt werden können. Ein Mensch vertraut einem KI-System, etwas zu tun. Es fehlt an Vorhersagbarkeit, daher ist die Situation von Unsicherheit und eventuell sogar von grossem Risiko geprägt. Der Mensch macht sich verletzlich, wenn er das Risiko eingeht, sich auf die Maschine zu verlassen und danach zu handeln. Das KI-System performt nicht, das Ziel der Mensch-Maschine-Interaktion ist nicht erreicht und der Mensch wird verletzt.

Technische Schwachstellen beschädigen vielleicht eine Maschine, aber verletzt wird am Ende ein Mensch. Die Maschine *leidet* im eigentlichen Sinn nicht. Daraus kann geschlossen werden, dass die Vertrauensbeziehung in der Mensch-Maschine-Interaktion unidirektional ist: Nur der Mensch kann vertrauen, kann Risiken eingehen und verletzt werden. KI-Systeme sind durch technische Schhwachstellen verwundbar, leiden jedoch nicht. Nur der Mensch leidet und das vielleicht sogar in doppelter Hinsicht: Ein Nutzer, der sich verletzt hat, da ihm geschadet wurde und die Entwicklerin, die sich verletzt hat, weil sie sich schuldig fühlt und sich verantwortlich gemacht hat. Vielleicht ist die Vertrauensbeziehung in der Mensch-Maschine-Interaktion doch nicht so unidirektional?

ZEIT FÜR EINEN PARADIGMENWECHSEL?

Während Vertrauen nur bei menschlichen Akteuren entsteht, zeigt sich die Verletzlichkeit bei allen Akteuren. Und dies in unterschiedlichen Formen, die sich auf noch unbekannte Weise beeinflussen. Bringen wir als Beispiel einen *Hacker* ins Spiel, der absichtlich versucht, Schwachstellen der Software auszunutzen, um einer Person zu schaden. Oder eine Firma, die böswillig *manipulative Designstrategien* entwickelt, um Vertrauen zu fördern. Schnell merken wir, wie die Mensch-Maschine-Interaktion an Komplexität gewinnt. Einfacher wäre vielleicht die Betrachtung aus Perspektive der Schwachstellen. Dann wirkt das KI-System eigentlich als eine Art notwendiger Zwischenhändler zwischen den menschlichen Akteuren. Denn eine Schwachstelle in der Maschine funktioniert am Ende nur zusammen mit der Schwachstelle Mensch.

Diese neuartige Idee des Managements, welche sich auf Verwundbarkeiten fokussiert, fusst auf den folgenden Thesen:

1. Der Mensch ist verwundbar, egal auf welcher Seite des KI-Systems er steht

2. Der Mensch hat Schwächen, die ihn verwundbar machen: z.B. zu viel Vertrauen (Overtrust) oder die kognitive Verzerrung, dass Maschinen immer perfekt funktionieren (Automation Bias)

3. Das KI-System ist verwundbar, weil es entweder schlecht gebaut (vielfältige technische

Schwachstellen) und/oder schlecht genutzt wird (z.B. technische Schwachstellen werden ausgenutzt)

4. Die Leidtragenden sind immer die Menschen: Negative Konsequenzen, Schuld, Verantwortung etc.

Das Ziel von vertrauenswürdiger KI ist negativen Konsequenzen zu minimieren. Jedoch ist es das Wagnis wert, einen *Paradigmenwechsel* vorzuschlagen: Weg vom Fokus auf Vertrauen und Vertrauenswürdigkeit, hin zum Fokus auf Verwundbarkeit. Daraus könnte eine Sicht auf die KI-Systeme entstehen, die ganzheitlich die Verwundbarkeit von Menschen und Maschinen betrachtet. Denn weder Mensch noch Maschine funktionieren jemals perfekt, auch wenn uns das Hirn oder Werbung manchmal vorgaukeln. Wir müssen ständig wachsam sein und – um im Tech-Jargon zu bleiben – ständig patchen. Das betrifft einerseits die IT Systeme, aber andererseits auch unser menschliches Vertrauensniveau.

FAZIT

Die Vision ist Paradigmen für ein ganzheitliches *Verwundbarkeits-Management* aufzustellen. Leitlinien zur Verwundbarkeit zu entwickeln, scheint ein visionäres Unterfangen. Es gibt viel Spielraum bei der Auslegung und vielleicht wären Leitlinien auch zu starr. Das entspricht nämlich nicht der Tatsache, dass die Vertrauensbeziehung zwischen Mensch und Maschine ein dynamischer, kontinuierlicher Prozess ist. Fortlaufend müssen die Stellschrauben der Beziehung überwacht, überdacht, und geflickt werden. Der Fokus auf die Schwachstellen von Mensch und Maschine hat das Potenzial ein besseres Verständnis und bessere *Handlungsempfehlungen* herauszugeben, damit wir KI-Systeme in Zukunft effektiv, nachhaltig und vor allem sicher nutzen können.

Marisa Tschopp

ABKÜRZUNGEN SIND OFT EINE HERAUSFORDERUNG

Bildquelle: https://pixabay.com/images/id-7247831/

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