MUSletter

August 2023

We share knowledge.

Editorial

■ Werner Widmer

Das Thema Datensicherheit beschäftigt uns seit Jahren. Immer häufiger müssen wir zur Kenntnis nehmen, wie leichtsinnig oder gar fahrlässig mit unseren persönlichen Daten umgegangen wird.

Spätestens seit Ende Mai 2023 ist der Name Xplain wohl den allermeisten bekannt. Bei einem Hackerangriff sind dieser Firma hochsensible Daten von Bund, Kantonen und Polizei geklaut worden, die gar nicht auf den Xplain Servern hätten sein dürfen.

MUS Mitglied Paul Hösli hat mich auf einen spannenden Artikel bei «inside IT» hingewiesen, der einen interessanten Blick hinter die Kulissen bei Xplain erlaubt. Der Security Experte Christian Folini hat uns die Erlaubnis gegeben, seinen Artikel im MUSletter wieder zu geben.

• • •

Aus einem andern Blickwinkel beleuchtet Datenschutz-Experte Joachim Schmitz das Thema. E-Mobilität gewinnt an Bedeutung. Elektro-Fahrzeuge sollen einen massgeblichen Unterschied bewirken und eine Realisierung der Klimaneutralität bis zum Jahr 2050 ermöglichen. Öffentliche Ladestationen bergen aber zahlreiche Sicherheitsrisiken. Sein Artikel beleuchtet, wo Fallstricke und Gefahren bei der Nutzung der Strom-Zapfsäulen lauern und welche Schutzmassnahmen sich ergreifen lassen.

• • •

Und dann gibt es noch die alltäglichen Phishing Versuche per E-Mail, mit deren Hilfe zwielichtige Gestalten versuchen, an unsere Daten oder an unser Geld zu gelangen. Ein paar Beispiele aus meinem Posteingang stelle ich euch hier vor.

En schöne 1. August! ■

Leserbrief

■ Thomas Kägi

In zwei Beiträgen im MUSletter ist Apples «Mail» recht negativ kommentiert worden. Ich erledige meine E-Mail-Korrespondenz seit langem mit diesem Mail Client, wurde aber durch die erwähnten Artikel hellhörig.

An «Mail» gefielen mir vor allem die «Regeln», mit denen sich E-Mails in bestimmte Postfächer ablegen lassen und Spam-Filter sehr flexibel eingerichtet werden können. Der Spamfilter meines Providers Solnet ist weniger flexibel – nur ganze Domains können so blockiert werden.

In letzter Zeit hat die Spam-Flut stark zugenommen, sie werden raffinierter und sind deshalb schwieriger zu filtern. In den letzten Wochen kommen ständig Spams, deren Absender «@nl." enthalten, was ich als Regel so definiert habe, dass sie gleich gelöscht werden sollten. Werden sie aber nicht! Entweder landen sie im Postfach für Spam, oder sogar im normalen Posteingang.

Nachdem ich auch mehrere Spams mit TLD «in» erhalten habe, definierte ich eine entsprechende Regel. Wie immer nach der Eingabe einer neuen Regel fragte «Mail», ob diese auch gleich auf alle bereits abgelegten Mails angewendet werden solle, was ich bestätigte. Und siehe da, nicht nur die neue Regel wurde angewendet, sondern alle gesammelten «@nl.-Mails» wurden ebenfalls gelöscht. Das Programm erkennt die entsprechenden Mails also sehr wohl, aber vergisst den Filter bei ankommenden Mails anzuwenden. Ich hatte das zwar schon vor längerer Zeit festgestellt. Aber erst mit der stark wachsenden Spam-Flut wurde es jetzt so störend, dass ich nach einer Alternative suchen muss. Danke für die Hinweise in den erwähnten MUSletter-Artikeln. ■

LocalTalk

Der LocalTalk findet neu immer am Mittwoch statt!

Die Veranstaltungen sind «hybrid», sie finden vor Ort statt oder man kann sich per Zoom einwählen und von zuhause aus teilnehmen. Hier die nächsten Anlässe.

Mittwoch 9. August 2023
ab 18.45 Uhr Apéro vor Ort
ab 19.15 Uhr Einwahl bei Zoom
ab 19.30 Uhr Vortrag

Ort: Ellens Garten, Reservoirstrasse, Basel – oder zuhause mit Zoom.
Dieser LT findet nur bei schönem Wetter im Garten statt. Über die Durchführung wird kurz fristig entschieden. Es werden alle per Rundmail informiert. Genauere Angaben bitte bei Ellen (ekuchinka@mus) nachfragen. Bei Schlechtwetter findet der LT wie gewohnt bei Gruner AG, St. Jakobs-Strasse 199, Basel statt.

Thema: Shoppingfallen vermeiden
Im heutigen LT besprechen wir, wie wie man Shoppingfallen im Internet vermeidet. Da gibt es so einiges zu beachten.

Weitere Daten:
6. September, 11. Oktober

Wir freuen uns auf eine rege Teilnahme an diesen Veranstaltungen.
Ellen Kuchinka und Pit Hänger

Weitere Infos
http:/www.mus.ch/lt-basel
ekuchinka@mus.ch
pit.haenger@mus.ch

Mehr Schein als Sein bei Xplain

Kleider machen Leute, das ist auch bei der IT-Security nicht viel anders. Wie man vom "Äusseren" eines IT-Dienstleisters auf sein Inneres schliessen kann, erläutert Security-Experte

■ Christian Folini

Es gab eine Zeit, da warfen gewiefte Chefs bei einem Bewerbungsgespräch zunächst einen Blick auf die Schuhe des Bewerbers. Sie taten dies, weil sie glaubten daran ablesen zu können, ob sie es mit einer gewissenhaften Person zu tun haben. Diese Zeiten sind zumindest in der Informatik vorbei. Und doch gibt es Situationen, in denen der äusserliche Eindruck fast das Einzige ist, was uns bei der Bewertung der Seriosität eines Gegenübers helfen kann.

Banken sind sich dessen bewusst und achten bei der Wahl ihrer Standorte auf gute Nachbarschaft. Am liebsten quartieren sie sich in einem gediegenen Gebäude an bester Lage ein. Ein wenig repräsentativer Eingang neben einem Kebab-Stand wird als Hauptsitz normalerweise vermieden. Auch die Firma Xplain in Interlaken hat ihren Hauptsitz in einem solchen gediegenem Gebäude. Sie setzt es auf der Webseite fotografisch in Szene.

Architektonisch scheint also alles in Ordnung bei Xplain. Aber wie sieht es mit dem digitalen Äusseren aus? Sehen wir etwas, was uns Rückschlüsse auf die Cybersicherheit der Firma machen liesse? Ist die Firma in der Lage, ihre Server sicher zu konfigurieren? Setzt sie überprüfbare Best Practices korrekt um und spielt sie Updates auf öffentlich zugänglichen Servern zügig ein? Und wenn wir etwas in dieser Richtung bemerken, stützen diese Erkenntnisse unsere Bewertung der Firma oder zwingen sie uns, die positive Erscheinung, welche die Firma uns mit ihrem sonstigen Auftritt vermittelt, zu korrigieren?

Äusserer Eindruck zählt

Wenn die Öffentlichkeit die Cybersicherheit einer Firma bewerten will, dann bleibt ihr tatsächlich kaum etwas anderes übrig, als auf den äusseren Eindruck zurückzugreifen. Es ist in der Schweiz unüblich, dass Firmen der Allgemeinheit gegenüber Rechenschaft über ihren Security Track Record ablegen. Falls Penetration Tests durchgeführt werden, behält man die Ergebnisse geheim und falls Zertifizierungen vorhanden sind, dann bleibt doch die Unsicherheit zurück, ob die Vorgaben der Zertifizierung auch wirklich gelebt werden. Auch Xplain CEO Andreas Löwinger erklärte vor ein paar Jahren, dass man sehr zurückhaltend kommuniziere.

Genaueres könnte man als uneingeladener Sicherheitsforscher mit einer Tiefenbohrung herausfinden, aber ohne vorherige Absprache verbietet das Strafrecht jede Überwindung von Schutzmassnahmen auf einem Server. Und so bleibt der Öffentlichkeit eben nur der äussere Eindruck, um festzustellen, wie es um die Sicherheitskultur einer Firma bestellt ist. Laien stehen für diese Bewertung eine Vielzahl von einfachen online Bewertungstools zur Verfügung. Genannt seien hier SecurityHeaders.com, SSLLabs.com, Observatory.mozilla.org oder Internet.nl. Sie alle sind intuitiv verständlich.

Mit Ausnahme von SSLLabs rapportierten alle diese Hilfsmittel für Xplain bis letzte Woche einen sehr schlechten Eindruck. Die Sicherheit der Webseite liess einiges zu wünschen übrig und wurde von SecurityHeaders.com mit einem "F" am unteren Ende der Skala bewertet. Mit einfachen Mitteln liess sich dann zeigen, dass sich die ungenügende Konfiguration der Webseite nahtlos auf anderen Servern der Firma weiterzog.

Xplain
homeland security, digital end-to-end

Das Zuhause von Xplain gemäss Firmenwebsite.

Drei Jahre lang ungepatchten Server betrieben

Ein für das Fedpol bereitgestellter Jira-Server konnte zum Beispiel über eine Man-in-the-Middle Attacke angegriffen werden. Das hätte es erlaubt, die Passwörter von Mitarbeitenden des Bundes allzu einfach abzugreifen. Zudem war der Server seit der Installation vor über drei Jahren nie mehr gepatcht worden. Ohne jedes Schamgefühl zeigte Xplain die Version von Atlassian Jira 8.7.0 auf der Loginseite des Servers.

Die besagte Version war im Februar 2020 erschienen und wurde von Jira innert einer Woche von der Version 8.7.1 abgelöst. Dieses Security-Update schaffte es aber nie auf den Server von Xplain und als letzte Woche eine Diskussion darüber auf Twitter entbrannte, verschwand der Server kurz darauf vom Netz.

Das äussere, sicherheitstechnische Erscheinungsbild von Xplain ist also ausge-

sprochen unseriös und verschlechterte sich weiter, als CEO Andreas Löwinger gegenüber 'Watson' darlegte, dass man in puncto Sicherheit keine zu hohen Ansprüche an Xplain legen dürfe, zumal die Firma lediglich als Software-Lieferant fungiere. Auch eine entsprechende Zertifizierung sei unnötig, da man ja keine Daten von Kunden verwalte. Dazu findet sich im Darknet allerdings der Gegenbeweis.

Bei Closed Source ist kein Review möglich

Die wahre Naivität hinter der Aussage des Chefs zeigt sich aber erst bei Überlegungen zur Sicherheit der von Xplain entwickelten Software. Das Unternehmen stellt an sieben Standorten in der Schweiz und im europäischen Ausland sogenannte "Home Land Security"-Software für Bund und Kantone her. Sie verkauft diese "Closed Source" an ihre öffentlichen Kunden. Faktisch handelt es sich dabei aber um eine Blackbox, denn ein vertiefter Security-Review von Close Source Software ist kaum möglich. Vielmehr wird die fertig paketierte Software nach der Lieferung auf den Servern des Bundes und der Kantone installiert und zur Verwaltung von sensiblen Daten eingesetzt.

Oder anders gesagt: Ein staatlicher Akteur, der es auf die Eidgenossenschaft abgesehen hat, braucht gar nicht die Firewalls des Bundes zu überwinden oder zu hoffen, dass jemand in Bern auf einen ungesicherten Link klickt. Einfacher ist es, die erklärtermassen laxen Sicherheitshürden bei Xplain zu überwinden und sich in die Xplain-Software einzuschleichen. Er wird sich alsbald als Teil dieser Software hinter den Firewalls des Bundes in einem geschützten Netz wiederfinden.

Das strukturelle Problem des Bundes in diesem Bereich nennt sich Supply Chain Security. In Interlaken ist das offenbar auch 2023 kein Begriff, oder Herr Löwinger würde sein Herz nicht so offen auf der Zunge tragen. Respektive, er würde davor zurückschrecken, die für einen Angriff infrage kommenden Geheimdienste durch so unüberlegte Aussagen in der Presse auf seine Server einzuladen.

Dem Bund fehlt die Security-Brille

Xplain und Löwinger können nur deshalb seit Jahren so auftreten, weil beim Bund niemand mit einer sicherheitstechnischen Brille hinschaute oder auch nur genau zuhörte, wie fahrlässig der Lieferant sich äussert.

Der Delegierte des Bundes für Cybersecurity Florian Schütz betonte kürzlich in einem Interview, dass die Daten bei Xplain und nicht beim Bund abgeflossen seien. Oder anders gesagt: Die Schuld liegt nicht in Bern, sondern in Interlaken.

Wie kann es aber sein, dass es bei den vom Datenabfluss betroffenen Behörden wie der eidgenössischen Zollverwaltung, den zahlreichen Kantonsverwaltungen und auch beim Fedpol niemandem auffiel, dass der Lieferant sicherheitstechnisch einen sehr schlechten Eindruck machte? Offenbar gaben Fedpol-Mitarbeitende über Jahre hinweg ihre Passwörter auf einem ungepatchten Xplain-Server ein, ohne sich um die veraltete Versionnummer auf der Eingabemaske zu kümmern. Das ist ein fahrlässiges Verhalten und lässt sich nur durch eine mangelnde Sicherheitskultur auf Seite des Bundes erklären. Genau dies hat Lukas Mäder vor Wochenfrist in seinem Kommentar in der 'NZZ' moniert und wir können es hier an einem konkreten Gegenstand festmachen.

Wie sähe eine angemessene Sicherheitskultur aus? Es würde bedeuten, dass die Mitarbeitenden des Bundes sich weigern, ihre Passwörter auf einer schlecht gesicherten Eingabemaske einzutippen und dass die Verantwortlichen umgehend eine Behebung der belegbaren Schwachstellen von Xplain verlangen.

Ein gediegenes Gebäude?

Die verschiedenen, unter anderem von SecurityHeaders.com monierten Probleme sind für Laien nicht zu durchschauen. Das müssen sie aber auch gar nicht. Es reicht die Meldung: "Liebes NCSC, wir haben hier eine Seite, die mit 'F' bewertet wird. Wir verstehen zwar nicht genau, was das bedeutet, aber könntet ihr mal einen Blick darauf werfen?" Es wäre dann die Rolle des NCSC, so einem Anfangsverdacht nachzugehen.

Diese Meldungen sind aber nach allem, was wir wissen, unterblieben, oder sie sind versandet, was natürlich dem Bund und seiner Sicherheitskultur ein noch schlechteres Zeugnis ausstellen würde.

Wenn nun aber die Kunden jede Sensibilität für Sicherheit vermissen lassen, ein angemessener Schutz der eigenen Firma kein Zuschlagskriterium bei Ausschreibungen darstellt und auch vertraglich keine Standards verlangt werden, dann verhält sich Xplain so rational wie jedes andere gewinnorientierte Unternehmen: Sie alle liefern genau das Minimum an Sicherheit, das man bei Bund und Kantonen von ihnen verlangt.

Wo die Sicherheitskultur auf Kundenseite fehlt, da spielt die von aussen gut sichtbare Cybersicherheit der Firma keine Rolle und Xplain kann sich bei der Pflege ihres Äusseren darauf beschränken, in einem gediegenen Gebäude zu residieren.

In frontaler Perspektive sieht die Fassade des Firmensitzes von Xplain übrigens etwas anders aus als auf der Webseite inszeniert. Während man dort den Bildausschnitt möglichst vorteilhaft wählte, sieht man auf einem Foto von vorne das Türschild von Xplain am Anbau auf der linken Seite (gelbe Markierung) gleich neben einem Kebab-Stand. ■

Ich wollte nur schnell laden – Welche Sicherheitsrisiken sich in E-Ladesäulen verbergen

Wo lauern die Fallstricke und Gefahren bei der Nutzung der elektronischen Zapfsäulen und welche präventiven Schutzmassnahmen lassen sich ergreifen? Informationen und Ratschläge präsentiert der Datenschutzexperte

■ Joachim Schmitz

Egal ob Tesla oder E-Roller, die Alternativen zu konventionellen Verbrennern erfreuen sich auch in der Schweiz einer grossen Beliebtheit. Im Jahr 2022 knackte die Anzahl neu zugelassener Fahrzeuge die Rekordmarke von 40 000 Fahrzeugen und erreichte somit einen prozentualen Anteil von knapp 15 Prozent. Vertreter der Autoindustrie beklagen einen Mangel an öffentlichen Ladestationen für Elektrofahrzeuge. Doch die Problematik liegt nicht nur in der geringen Anzahl an Ladestationen, sondern auch in mangelnden Sicherheitsvorkehrungen. Datenschützer kritisieren etwa den laxen Umgang mit personenbezogenen Daten, die bei der Freischaltung der öffentlichen Ladestationen in Umlauf geraten.

Problematik mit dem Datenschutz

Bei der Nutzung der öffentlichen Ladesäulen werden während des Bezahlvorgangs Daten transferiert, die mitunter Name, Adresse, Fahrzeuginformationen, Kreditkarten- und Bankinformationen enthalten können. Eine unsachgemässe Handhabung dieser Daten kann ein Risiko für den Fahrzeughalter bedeuten.

Um die Gefahren besser ins Bewusstsein zu rufen hilft es, sich näher mit dem Ladeprozess vertraut zu machen. Während einer Aufladung steht das Fahrzeug in stetiger Kommunikation mit der Ladesäule, die Informationen wie etwa den Ladestand anfragt. Diese Daten sowie die Bezahldaten werden nach Abschluss der Transaktion im Speichersystem der Ladesäule gesichert. Verfügt die Ladesäule nun über einen USB-Port für etwaige Wartungsarbeiten, können sich Unbefugte bei fehlenden Sicherheitsmassnahmen Zugriff zu den gesicherten Daten verschaffen.

Selbst sicher wirkende Technologien wie Plug & Charge besitzen offene Schwachstellen. Hier startet das Anstecken des Ladekabels den Ladevorgang. Da keinerlei Funkchip oder Drahtlos-Karte mehr notwendig ist, scheint der Prozess für den Verbraucher sicher. Die Datenweiterleitung findet hier nämlich über eine sichere lokale Verbindung statt. Allerdings ist auch hier die Auslesung der Daten möglich, zum Beispiel mit einem DVBT-Stick. Hierzu ist für Hacker kein direkter Zugriff auf das Auto notwendig. Beim Laden

Ladesäule mit Typ-2-, Combo-2- und CCHdeMO-Anschluss. (Quelle: Wikipedia, User Hadhuey)

erfolgt die Kommunikation zwischen Ladesäule und Fahrzeug über ein OCPP-Protokoll, das von technikaffinen Nutzern leicht umgangen werden kann.

Schutzmassnahmen vor Datenmissbrauch

Ladestationen werden in der ganzen Schweiz von verschiedenen Anbietern betrieben. Zu den gängigen gehören etwa eCarUp, evpass, Swisscharge, TCS eCharge und MOVE. Trotz Datenschutzverordnung sollten sich Nutzer*innen vorab über die Datenschutzbestimmungen der jeweiligen Ladesäule und deren Betreiber vertraut machen.

Obwohl der Komfort mancher Ladeapplikationen auf den ersten Blick lockt und zahlreiche Vorteile für Kunden bietet, können derartige Anwendungen nutzerbezogene Daten wie Standortinformationen sammeln und während des Ladevorgangs weiterreichen. Auf diese Weise ist die Erstellung eines persönlichen Bewegungsprofils oder Nutzungsverhaltens möglich. In der Regel ist die Datenhandhabung intransparent und für den Nutzer kaum einsehbar.

Folgende Massnahmen helfen, sich vor Betrug an der Ladestation zu schützen:

1. Die Ladesäule vor der Nutzung inspizieren. Bei äusseren Beschädigungen ist die Nutzung der Station riskant.
2. Der Ladechip lässt sich auch durch Kleidung hindurch auslesen und sollte nicht offen herumliegen.
3. Die Rechnung auf Parameter wie Ladedauer, Lademenge, Zeit und Ort prüfen.
4. Die Zahlung mit dem iPhone ist sicherer als per NFC-Karte oder Funkanhänger.

Fazit

Durch intransparente Systeme haben Nutzer*innen nur beschränkte Möglichkeiten, über ihre eigenen Daten zu walten. Durch Vergleich der Datenschutzbestimmungen verschiedener Anbieter und durch die Einhaltung einiger Vorsichtsmassnahmen lässt das Risiko für einen Datenklau auf ein vertretbares Minimum senken. ■

Combo-2 Anschluss im Auto. (Quelle: Wikipedia)

Achtung Phishing!

Die Phishing Versuche via E-Mail werden immer ausgefeilter. Hier ein Beispiel, auf das ich selber reingefallen bin.

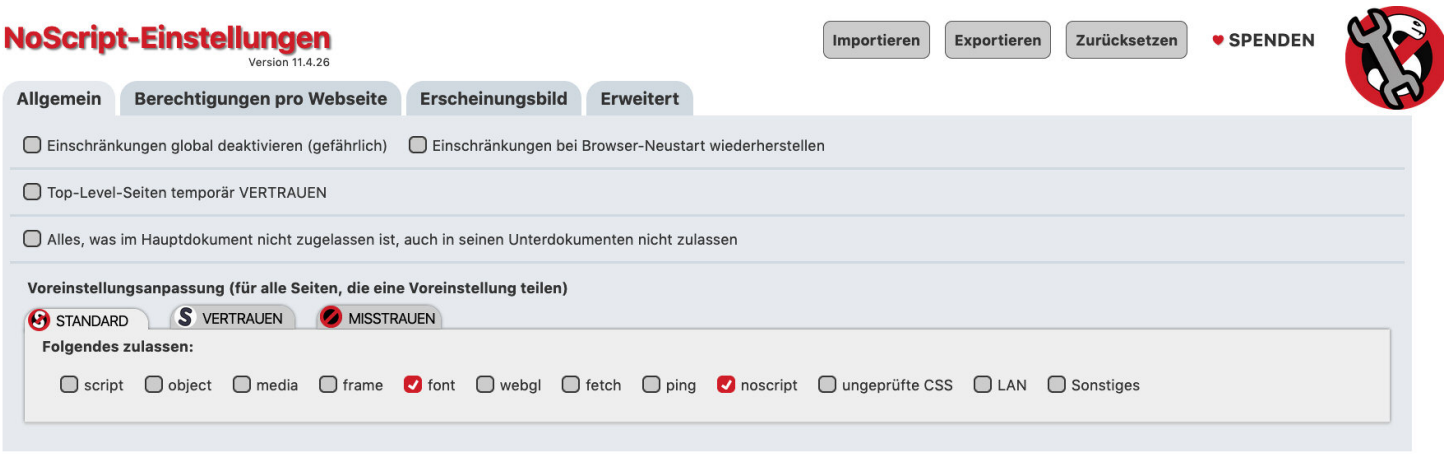
■ Werner Widmer

Am 4. April 2023 trudelt ein E-Mail ein mit dem Hinweis auf die neue Swisscom Rechnung. So weit nichts Besonderes, das passiert monatlich so um den 5. herum. Also Klick auf «Rechnung einsehen», damit gelangt man auf den Swisscom Server und kann die Rechnung herunterladen oder online bezahlen. Aber der Browser meldet einen Verbindungsfehler. Auch das ist nicht ungewöhnlich, da mein Firefox mit der NoScript Erweiterung geschützt ist, die grundsätzlich alles sperrt, was ich nicht explizit erlaube. Stutzig werde ich erst, als auch nach Freischalten verschiedener Parameter die Verbindung nicht gelingt. Ich maile die Fehlermeldung an Swisscom und kümmere mich um andere Dinge.

Zwei Tage später kommt ein E-Mail von Swisscom, das mir erneut eine Rechnung ankündigt. Weil der Betrag geändert hat werde ich stutzig und schaue mir die Sache genauer an. Erst jetzt und nur bei genauem Hinsehen fallen mir einige Ungereimtheiten auf. Eines der beiden Mails ist ein Fake - aber welches? Und woran kann ich das erkennen?

Die wichtigste Prüfung gleich zuerst: Den Mauszeiger über der Taste «Rechnung einsehen» positionieren ohne zu klicken, nach etwa einer Sekunde wird die Hyperlinkadresse eingeblendet (siehe Screenshots). Der Link im ersten Mail deutet auf eine anonyme IP-Adresse, der Link rechts auf den Swisscom Server. Weiter ist das Mail rechts signiert von Secure Mail Gateway, ein Aufwand, den Betrüger (noch) scheuen. Ferner ist beim echten Mail unten die Kundennummer eingeblendet, und auf <mus@mus.ch> gehen normalerweise keine Rechnungen ein.

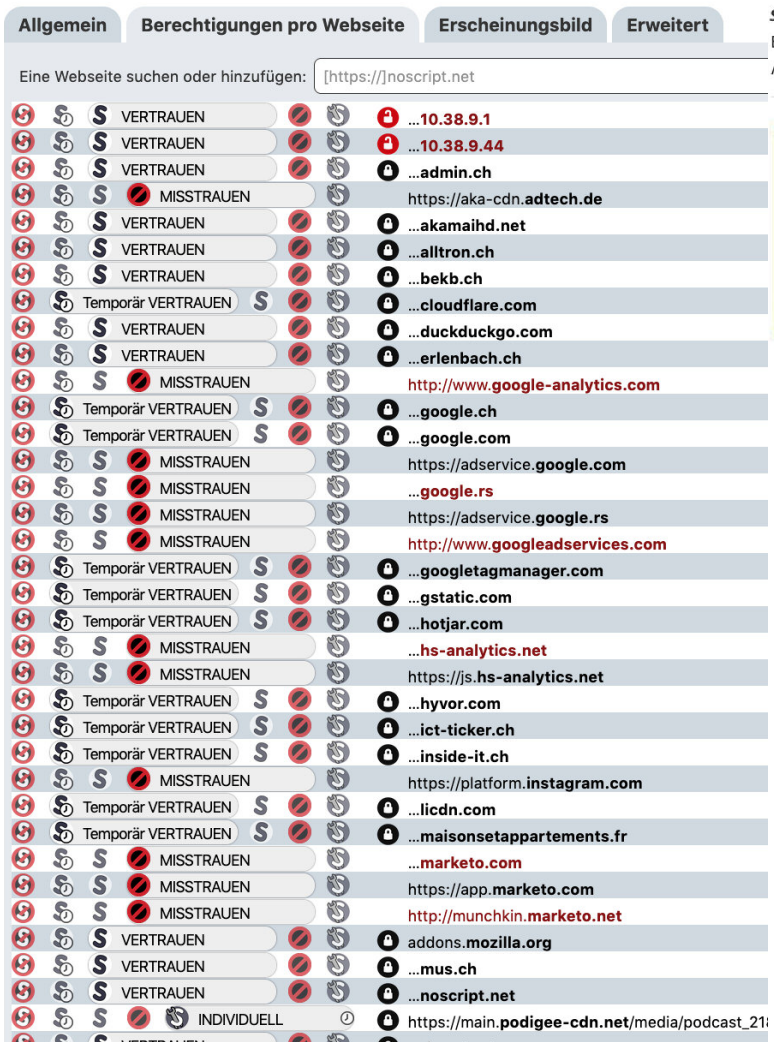
Aber wie gesagt, in der täglichen Routine sind mir diese Details nicht aufgefallen. Das falsche Mail ist täuschend ähnlich, der Text ist identisch, die Schrift stimmt weitgehend mit dem Original überein. Und der Versand erfolgte im richtigen Zeitraum. Fazit: Das erste Mail war ein gut gemachter Phishing Versuch. Ohne NoScript, das die Verbindung blockierte, wäre ich den Gaunern vielleicht voll auf den Leim gekrochen. ■



Die NoScript Erweiterung für Firefox ist eine mächtiges Werkzeug, um den Browser zu stählen.

Mit meinen strikten Grundeinstellungen (oben) ist erst mal gar nichts erlaubt ausser HTML Code. Damit lassen sich Schadcode und Werbung weitestgehend fernhalten. Allerdings funktionieren viele Webseiten dann nicht wie vorgesehen, was oft aber nicht stört bzw. sogar gewollt und angenehm ist: kein Blinken und Flimmern, keine fliegenden Banner etc., man kann in Ruhe den Text lesen. Bei Bedarf lassen sich mittels Feintuning die benötigten Funktionen pro Webseite individuell steuern.

Unten rechts: Noch ein Beispiel eines Phishing Mails. Grundsätzlich ist bei QR Codes Vorsicht geboten. Oft wird man auf dubiose Websiten gelockt, gelegentlich zahlt man gar fremde online Bestellungen in einem Webshop ohne es zu merken – bis dann die Kreditkartenabrechnung ins Haus flattert. ■



Bilder aus dem Sekretariat

We share knowledge.

Wo Aktenberge sich erheben ... Hier werden archivierte Akten der Jahre 2002 bis 2012 entsorgt

iPhone Bilder im Juli

We share knowledge.

Blick von der wolkenverhangenen Rigi über den Zugersee. 26.7.23, 16.08 Uhr. Aufnahmen mit dem iPhone 8. © W. A. Widmer, Erlenbach.
Züri-Fäscht 2023. Das grösste Fest der Schweiz und das sechstgrösste der Welt, noch vor dem Karneval von Rio (Eigenwerbung des OK).