

## Corona-Presskonferenz der ...Anzeiger Redaktion vom 8. April 2020

Es nehmen teil:

Ulrich-Nikolaus ter-Nehmungssprecher, ...Anzeiger-Unternehmenssprecher  
Ian Nolan Secure, renommierter Computer-Experte

---

**U.N. ter-Nehmungssprecher:** Guten Abend miteinander. Ich begrüsse Sie zu dieser ausserordentlichen Pressekonferenz zwischen den regulären Corona-Presskonferenzen des ...Anzeigers während der Corona-Krise. Anlass für diese PK ist ein Angebot von Ian Nolan Secure, Computer-Experte. Sehr renommiert. Herr Secure hat uns angeboten, über Themen der Informationstechnologie zu sprechen. Diese erfreuen sich aufgrund der Massnahmen der einzelnen Regierungen einer ganz neuen Aktualität. Bevor wir die Runde für Fragen öffnen, geben wir wie üblich die aktuellen Zahlen innerhalb der ...Anzeiger-Redaktion. Es sind nicht noch nicht alle Resultate aus allen Kantonen eingetroffen, aber soweit bekannt sind keine neuen Fälle eingetreten. Somit haben wir nach wie vor null Infizierte. Wie wir alle wissen, sieht es weltweit anders aus. Allen Erkrankten wünschen wir eine baldige Genesung.

Nun aber zu Mr. Secure. Vielleicht können Sie sich mit einem kleinen Eingangsstatement kurz vorstellen und Ihre Beweggründe darlegen, warum Sie heute Abend hier sind.

**Ian Nolan Secure:** Nun äh, ich habe erst gerade von der Krise erfahren. Per Zufall. Ich war am Computer, as Usual. Ich gehe einmal die Woche einkaufen, und sonst bin ich am Arbeiten. Ich mag keine Menschen. Also war ich überrascht, dass mein Leben von anderen als "Lock-down" bezeichnet wird. Wie auch immer. Ich dachte es sein mal Zeit die Leute über IT-Security aufzuklären, da viel Irrglauben und falsche Informationen vorherrschen. Der Anzeiger ist eines der wenigen Medien, die keine Kurzarbeit machen (neben der Republik), das muss man unterstützen

**U.N. ter-Nehmungssprecher:** Über welchen IT-Background verfügen Sie?

**Secure:** Ich arbeite seit 30 Jahren im Sicherheitsbereich. Mit Computer beschäftigte ich mit seit den 90er Jahren. Ich habe da ein tolles Spiel auf dem Apple Plus entwickelt. Man konnte von einer Burg auf eine Andere schiessen, indem man die Weite und den Winkel eingibt. Ich frage mich, ob das heute noch jemand spielt

**ter-Nehmungssprecher:** Ich denke das wollen wir nicht weiter vertiefen. Vielen Dank erstmal. Ich eröffne die Runde für Fragen.

**Konrad Gwunderlin:** Guten Tag Herr Secure: Welche Sicherheitsmassnahmen gelten im Home Office? Und zweite Frage, ich habe gehört es gibt Arbeiter, die sich via RSA Token ins interne Netz einloggen, Für wie sicher halten Sie den RSA-Token?

**Secure:** Zur ersten Frage 1: Es gibt ja 10 Sorten von Firmen, zum Thema Home Office. Diejenigen, die meinen Home Office im Griff zu haben, und jene die es nicht im Griff haben. Es stellte sich dann heraus, dass die Firmen gar nicht vorbereitet waren. Auch grosse Unternehmen in der Schweiz waren überfordert. Die Einen haben gemerkt, oh wir haben nur VPN-Lizenzen für 300 Benutzer, aber jetzt arbeiten 2'000 von zu Hause. Zur Sicherheit, wenn das Gerät gut geschützt wäre, könnte man von zu Hause genau gleich weiterarbeiten wie im Büro. Wussten Sie übrigens, dass der "Wäre", "Könnte" und "Hätte" drei Brüder waren? Die haben immer viel gemacht und standen am Ende mit leeren Händen da. Genug geredet, sie wollten ja Sicherheitsmassnahmen. Machen wir es einfach. Das Notebook der Firma ist ein Firmengerät. Da arbeitet nur der Mitarbeiter dran. Nein, das neue Game für die Kinder wird nicht installiert.



Nein, Lebenspartner dürfen das Gerät nicht benutzen, weil deren Firma kein Notebook übrig hatte. Nein, der freie Zugang von Pornhub darf auf dem Gerät nicht genutzt werden. ... Ich würde das Tastatur-Layout auf Russisch einstellen, das erspart Ärger mit Malware.

**Secure:** Zur zweiten Frage: Gut, ich habe ja überhaupt gar kein Mitleid mit Leuten, die RSA Tokens einsetzen. Das ist proprietäre symmetrische Krypto, "unveröffentlicht", ein "Geschäftsgeheimnis". Das alleine reicht schon, um die in meinen Augen völlig für jeden Einsatz irgendwo zu disqualifizieren. Aber dann wurde RSA gehackt und die Angreifer haben die Seeds rausgetragen. Das kam 2011 raus. Und es hiess damals, das seien die Chinesen gewesen. Seit dem warten alle darauf, dass jemand zugibt, über RSA-Tokens gehackt worden zu sein. Wer immer noch RSA-Tokens einsetzt, der hat verdient, dass ich mit Popcorn auf den Rängen sitze und gehässig lache.

**Gwunderlin:** Anschlussfrage dazu, sagen wir mal sensible Daten wie diejenigen der Schweizerischen Post werden durch einen RSA-Token geschützt...

**Secure:** Nun, das kann man schon so machen... \*hust\* Wie vorher erwähnt, RSA Tokens waren in den 90er noch okay. In 2020 sollte man doch besser eine andere Lösung verwenden. Aber man weiss ja, die Post ist nicht immer pünktlich. Und wenn sie mal pünktlich sind, kriegen sie ein dreifaches Hurra.

**Loïc Navarro:** Bonsoir Monsieur Secure.

**Secure:** Good Evening

**Loïc Navarro:** (murmelt) War ja zu erwarten... (erhebt die Stimme) Apropos Home Office, Meetings finden ja nun grossmehrheitlich per Videokonferenz statt. Da hat sich ein Anbieter hervorgetan, nämlich «Zoom». Die App ist zuletzt mit negativen Schlagzeilen aufgefallen. Was für Schäden wurden schon angerichtet. Was raten Sie Firmen, welche Zoom verwenden? Welche Alternativen gibt es? Welche Daten hat Zoom von mir und meinen Angestellten und hat Zoom diese bereits weitergegeben?

**Secure:** Zu Zoom habe ich ein gespaltenes Verhältnis. Einerseits werden jetzt kleine Schwachstellen als Drama gehyped. Andererseits tritt Zoom die Privacy mit den Füssen. Die haben komischerweise Code im Programm entdeckt, dass Daten zu Facebook versendet. Was für ein bedauerliches Missverständnis. Wie konnte das nur passieren? Nun entweder machen sie gar keine Qualitätskontrolle (=schlecht) oder sie haben eine schlechte Ausrede parat, da sie mit dem Finger im Marmelade-Glas erwischt wurden.

Als Firma sollte man sich ein Risiko- und Threadmodell erarbeiten. Heinz und sein Bruder, die Lotto veranstalten, müssen nichts befürchten. (schweigt, denkt nach) Ausser die Abrechnung ist getürkt. Nun aber wenn ich mit sensitiven Daten handle, würde ich nicht Zoom oder sonst ein Cloud-Provider wie Teams brauchen. Ich würde ein «Jitsi-Server» selber betreiben. Sehe ich aber im Business-Einsatz nur selten, da man mit Geld auf das Problem wirft, sprich beim grossen Hersteller einkauft, statt kompetente Leute zu haben, die selber was bauen.

Zoom kann auf Kontaktdaten zugreifen, Nutzerverhalten auswerten (wie aktiv hat man zugehört) und andere Daten auf dem Client auslesen. Es ist nicht bekannt, dass Gespräche mitgehört werden. Ob Zoom Daten weiterverkauft, kann ich nicht sagen.

**ter-Nehmungssprecher:** Ja den «Jitsi-Server» kennen wir natürlich alle...

**Secure:** Es gibt da eine Liste für «Jitsi-Server» für Interessierte: [Hier Klicken](#). Sogar die Uni Freiburg betreibt einen solchen Dienst.

**Gwunderlin:** Andere Frage, für wie sinnvoll halten Sie den Einsatz der Pepp-PT App im Kampf gegen Corona? Und zweitens, es wird häufig von Tracking und Tracing Apps gesprochen, was ist der Unterschied?



**Secure:** Wenn die Pepp-PT App wirklich die Ansprüche an den Datenschutz halten kann und sicher umgesetzt wird, dann besteht die Chance, dass die App freiwillig genutzt wird. Es braucht mindestens 60% Prozent der Bevölkerung, die mitmacht. Und die muss es von sich aus wollen, sonst bringt es nichts. Ich hoffe niemand kommt auf die Idee man könnte eine App von militärnahen Kreisen aus der USA oder von Ex-Militärs aus Israel einsetzen.

Beim Tracking werden die Mobilfunkdaten ausgenutzt, was jetzt schon passiert. Swisscom arbeitet unter anderem schon seit Jahren mit Verkehrsdatenprovider zusammen, um Staudaten zu liefern. Wussten sie nicht? Tja, hätte man im aktuellen DSG einen Opt-In-Zwang, hätten sie dazu zusagen müssen. Jetzt müssen Sie irgendwo das Formular der Swisscom finden, um dem zu widersprechen. Laut Aussage des BAG werden keine Standortdaten, sondern lediglich Analysen und Visualisierungen, die darunterliegenden Daten seien anonymisiert. Das BAG weigert sich jedoch die Verfügung dazu herauszugeben... Die Digitale Gesellschaft hat ein Verfahren gegen das BAG gemäss Öffentlichkeitsgesetz (BGÖ) eingeleitet und nach ein paar Tagen wurde dann die Verfügung publiziert. Beim Tracing werden per Bluetooth Kontakte ausgewertet. Der CCC hat da einen Anforderungskatalog erstellt, was eine solche App befolgen sollte: <https://www.ccc.de/de/updates/2020/contact-tracing-requirements>

**Navarro:** Da Sie das DSG ansprechen, Könnten wir nicht alle bei der Einführung der App beruhigter schlafen, wenn wir ein neueres Datenschutzgesetz als dasjenige von 1992 hätten? Wären meine Daten nicht sicherer, wenn der Bund mit der Revision nicht etwas vorwärts machen würde? Denken Sie der Bund will überhaupt vorwärts machen? Ist der Stillstand auf ein Versagen der Verwaltung zurück zu führen?

**Secure:** Es ist unverantwortlich wie hier Zeit verplempert wird. Aussagen wie "Datenschutz wird Unternehmen so viel Geld kosten" zeigen, dass man von der Thematik nichts verstanden hat. Wenn das Datenschutzgesetz der Schweiz von der EU als inkompatibel mit dem GDPR eingestuft wird, dann wird es viel viel mehr Geld kosten. Im schlimmsten Fall macht man dann kein Business mehr mit EU-Staaten. Zudem sollte im DSG vorgesehen sein, dass Unternehmen, die sich nicht an Datenschutz halten, richtig hart gebüsst werden. Sonst wird es nie funktionieren. Solange der EDÖB "Empfehlungen" aussprechen darf, wen kümmerts? Wenn ich ein Business mit Kundendaten habe, ich verdiene damit 10 Millionen. Die Daten nach DSG korrekt zu verarbeiten kostet mich eine Mio. und die Busse ist max. 200'000. Würden Sie die Mio. ausgeben? Natürlich nicht.

Bezüglich Verwaltung: Ich glaube es gibt zwei Fronten dort, die Einen die das DSG vorwärts treiben wollen und die Anderen, die von einem Moloch reden. Es ist immer einfacher alles kaputt zu reden, als selber etwas zu bauen. Es sollte langsam allen klar sein, dass wir hier Resultate brauchen. Und zwar ein anständiges DSG. Es ist für mich schwer verständlich, wenn man die Schweiz als "sicheren Datenhafen" sieht und gleichzeitig als einziges Land hier in Europa eine Vorratsdatenspeicherung betreibt. Die EU-Richtlinie wurde übrigens durch den Europäischen Gerichtshof als ungültig erklärt. Ich befürchte die Ratsmitglieder hören ein weiteres Mal auf die falschen Berater, wie schon beim Glücksspielgesetz.

Ein schärferes DSG gäbe uns die Möglichkeit uns zu wehren. Auch wenn missbräuchlich Marketing-Mails versendet werden, obwohl man dem Versand widersprochen hat. Es funktioniert nur, wenn man sündige Unternehmen büsst. Und zwar happig, nicht mit Portokassenbeträge. Solange wir die App freiwillig benutzen können, unterliegt es der informationellen Selbstbestimmung und das ist gut so. Ich schlafe schlecht, wenn wir dazu gezwungen werden und dazu noch eine Lösung der genannten Firmenkreise verwendet wird.



Falls das BIT selbst eine Lösung programmiert, dann kann ich auch nicht mehr schlafen, weil ich nicht aufhören kann zu lachen.

**ter-Nehmungssprecher:** Ganz kleiner Einschub, ich erhalte soeben die Meldung, dass die Notfallnummern im Kanton Freiburg nicht mehr erreichbar sind aufgrund einer Panne im Swisscom-Netz, was ist da los bei der Swisscom?

**Secure:** Überraschung. Das Telefon-Netz mit Notfallnummern wurde vom Ex-Monopolist kaputt gespart. Das rächt sich jetzt.

**Gwunderlin:** Halten Sie das für eine allgemeine Tendenz bei Ex-Monopolisten?

**Secure:** Nun, Konkurrenz belebt das Geschäft. Es gibt viele tolle Internetangebote, aber die Swisscom bedrängt die Provider. Dann macht die Swisscom falsche Aussagen oder verlangt zu viel Geld. Die Kleinen klagen. Am Ende gibts eine Busse für die Swisscom von der WEKO. Die ist lächerlich klein und der Markt ist kaputt. Dann gibt es da die Postauto Dienste. Da wurde auch gemauschelt. Bei Paket- und Briefdiensten wäre es auch interessant, wenn es mehr Möglichkeiten gibt. Ich kriege per UPS/DHL ein Paket aus der USA in zwei Tagen. Ein Paket von Digitec geht nach Frauenfeld, fährt einen Tag mit dem Pöstler rum, geht wieder nach Frauenfeld und dann erst nach Winterthur.

**Navarro:** Zurück zur IT, Thema Phishing. Es gibt leider auch zu Krisenzeiten Leute, welche die Panik ausnützen. Im Umfeld der Post gibt es Mailnachrichten, welche die Leute zu Zahlungen von Portokosten über Kreditkarte auffordern, was die Post natürlich nie von den Kunden fordern würde. Welche Aktionen sind Ihnen bekannt und wie kann man sich dagegen wehren?

**Secure:** Im Moment gibt es Informationen zu Corona, Klassiker wie Paket-Zustellung, Rechnung. Ich habe kürzlich einen KMU-Newsletter erhalten. Sah auch sehr suspekt aus. Grundsätzlich immer mit Common Sense an die Sache ran gehen und mit dem Grundsatz "Too good to be true". Es will ihnen jemand Geld schenken? Ja klar. Das Paket von DHL konnte nicht zugestellt werden? Haben sie denn ein Paket bestellt? Sie kriegen einen KMU-Newsletter obwohl sie alle Newsletter abbestellt haben?!

**ter-Nehmungssprecher:** Der Newsletter scheint Sie sehr zu beschäftigen...

**Secure:** Er braucht übermässig viel Zeit. Normalerweise kann man ja einen Newsletter abbestellen mit einem Klick. Der Absender war aber sehr umtriebig. Auf dem Phishing-Portal war keine Abmeldemöglichkeit. Bei der Hotline wurde auf die AGB verwiesen. Als kritisch nachgefragt wurde, wurde gesagt, ja man kann dem Versand auch widersprechen. Als das getan wurde, kam drei Wochen später wieder ein Newsletter, man erhalte zwei Webstamps gratis! Wenn man zehn weitere kauft.

**ter-Nehmungssprecher:** Ich hoffe Sie gehen gegen diese betrügerische Firma aufs Härteste vor.

**Secure:** Es wäre ja toll, könnte man so ein Geschäftsgebahren dem EDÖB melden... aber was solls, der kann ja nur Empfehlungen aussprechen...

**Navarro:** Auch hier ein Versagen der Bundesverwaltung?

**Secure:** Man sollte endlich das DSG verabschieden. Aber nicht jetzt noch weichkochen lassen. Sonst muss sich die Bevölkerung selbst wehren. Vielleicht könnte man eine bekannte Grösse aus Winterthur einspannen. Man munkelt diese Person hat die Stadt Winterthur beschuldigt, Verkehrsteilnehmer mit einem gefährlich roten Licht aus sogenannten Radaranlagen zu gefährden! Und er hat eine Antwort erhalten!

**U.N. ter-Nehmungssprecher:** Vielleicht nochmal zum Thema suspekten Mailnachrichten. Ich erwarte ein baldiges Return of Investment aus Nigeria. Wann kann ich damit rechnen?



**Secure:** Der Prinz von Nigeria ist ein guter Freund von mir. Er schreibt seit Jahren E-Mails so, dass nur 0.5% der Absender darauf reinfallen. Das ist reine Absicht, damit nur die Dummen und Geldgierigen darauf regieren und keine Fragen mehr stellen, sondern überweisen. Gegen einen kleinen Unkostenbeitrag kann ich für Sie ein gutes Wort einlegen, um ihre Transaktion zu beschleunigen.

**ter-Nehmungssprecher:** Ich komme vielleicht nach der PK darauf zurück.

**Secure:** Haben Sie Revolut?

**ter-Nehmungssprecher:** Sie meinen diese App, die manchmal einfach so Konten von Nutzern sperrt? Und dann monatelang nicht wieder freigibt?

**Secure:** Sie meinen doch nicht die Kunden, die undurchsichtige Zahlungen für ihre Freunde durchführen? Und dann überrascht sind, dass eine Fraud Detection anschlägt? Wie schon Ueli sagt, unterschätzen sie die Banken nicht... Die haben sogar Meldelisten für Begriffe die in den Kommentarfelder bei Zahlungen verwendet werden.

**ter-Nehmungssprecher:** Gut, wir nähern uns dann langsam dem Ende. Gibt es noch Fragen? Scheint nicht der Fall zu sein. Haben Sie noch etwas auf dem Herzen Herr Secure?

**Secure:** Stay alert and secure kann ich da nur sagen

**U.N. ter-Nehmungssprecher:** Damit beschliessen wir die heutige Veranstaltung. Ich bedanke mich nochmals für den spontanen Auftritt von Ian Nolan Secure und seine informativen Stellungnahmen. Ich wünsche allerseits einen guten Abend. Der ...Anzeiger meldet sich am Karfreitag mit dem «Osteranzeiger» wieder. Die nächste Pressekonferenz findet am 18. April statt. bleiben Sie gesund!

