Studerus Technology Forum 2017

Anatomie eines Live-Hacks am Tefo 17

Do 23.11.2017 - 15:13 Uhr | Aktualisiert 23.11.2017 - 15:13
von Coen Kaat

Es ist wieder Tefo-Zeit. Distributor Studerus zeigt in Regensdorf, Zürich, in welche Richtung sich die Netzwerk-Branche entwickelt. Ein wichtiges Thema, wie bereits im Vorjahr, ist IT-Security. Ivan Bütler, CEO von Compass Security, zeigt, wie er im Auftag des SRF den Energieversorger EBL gehackt hat.

(Source: Netzmedien)

Das diesjährige Technology Forum ist eröffnet! Wie jedes Jahr lockte der Ruf des Distributors und Zyxel-Generalimporteurs Studerus zahlreiche Besucher ins Mövenpick Hotel Zürich-Regensdorf, um das Neueste rund um Netzwerk-Technologien zu erfahren.

Das Konzept des Anlasses sei dasselbe geblieben wie im vergangenen Jahr, sagte CEO Frank Studerus, als er die Gäste von der Bühne des Kongresssaals aus begrüsste. Die Technical Sessions der letztjährigen Tefo seien gut angekommen, weswegen auch dieses Jahr wieder ein Teil der Vorträge sich spezifisch an ein eher technisch orientiertes Publikum richten.

Frank Studerus, CEO und Gründer von Studerus AG. (Source: Netzmedien)

Die Technical Sessions sind gemäss Studerus sogar so gut angekommen, dass sie dieses Jahr in den normalen Vortragsräumen stattfinden. Im vergangenen Jahr hatte der Veranstalter dafür die kleinen Räume vorgesehen. Diese waren jedoch äusserst schnell ausgebucht, wie der CEO sagte.

Ebenfalls vom Vorjahr übernommen ist der Schwerpunkt auf das Thema IT-Security. Ganze acht Vorträge drehen sich heute um Cybersicherheit. Für den Distributor ist das Thema aktuell besonders spannend. Ende September hatte das Unternehmen die Firma BW Distribution aus Uster übernommen – und mit dem Unternehmen kam auch gleich die Security-Software von McAfee in das Portfolio von Studerus.

Das Tefo wird damit jedoch nicht zu einem IT-Security-Anlass. So adressierte Frank Studerus auch andere Trends, die er aktuell im Bereich Netzwerk erkennt. So werde etwa die Überwachung von Netzwerken ein stets wichtigeres Thema.

Monitoring wird immer wichtiger

"Wenn Freitag abends um 22 Uhr das Internet einer Ihrer Kunden aussteigt, merkt das jemand bei Ihnen? Wird wer informiert? Werden Massnahmen eingeleitet?", fragt Studerus das Publikum. Natürlich will niemand, dass man das erst am darauffolgenden Montag merkt. Für Systemintegratoren sei dies etwa eine Möglichkeit, Monitoring und Support als Dienstleistung anzubieten.

Der CEO wagt auch einen Blick in die Zukunft. "Wo geht die Entwicklung hin?", fragte er. "Durch Hardware alleine kann man sich heutzutage nur noch schwer differenzieren." Stattdessen geschehe die Abgrenzung gegenüber der Konkurrenz eher über die Usability. "Und da tut sich in letzter Zeit einiges", sagt Studerus.

Das Technology Forum 2017 fand wieder im Mövenpick Hotel Zürich-Regensdorf statt. (Source: Netzmedien)

Die Branche ist weit gekommen. So zeigte Studerus etwa ein Bild einer alten Tellnet-Benutzeroberfläche. Ein Bild, das den meisten Gästen im Publikum ein nostalgisches Lächeln herauslockte, bevor Studerus zum aktuellen Äquivalent wechselte: einem Web-GUI.

Aber auch das Web-GUI habe seine Einschränkungen für Netzwerkkonfigurationen. So könne man aus Sicherheitsgründen etwa nur aus dem LAN heraus auf Geräte zugreifen. Für Fernwartungen also denkbar ungeeignet.

Partner zeigen Zurückhaltung beim Thema Cloud

Eine Alternative sei etwa eine lokale Softwarelösung wie Zyxel One Network. Die sei gut für den Unterhalt und die Installation von Netzwerken – aber weniger für das Management. Eine weitere Alternative wären Apps. Im Consumer-Bereich kämen diese Bereits häufiger zum Einsatz. Im Business-Bereich eher weniger – ausser vielleicht für Alarme.

Der Trend gehe stattdessen eher in Richtung Cloud-Netzwerk-Konsolen wie etwa Zyxel Nebula. Derartige Lösungen böten einen Überblick über das gesamte Netzwerk. "Sie sind lokal wie ein Web-GUI, aber nicht stationär gebunden", sagt Studerus. Cloud-Konsolen eignen sich dank Remote-Zugriff daher auch für Fernwartungen.

Ein weiter Vorteil: Der Nutzer könne einfach unterschiedliche Netzwerke und auch Benutzer-Accounts damit verwalten. So könne der Administrator etwa auch Accounts nur mit Lesezugriff für seine Kunden einrichten.

"Wir spüren beim Thema Cloud aber noch Zurückhaltung bei den Partnern", sagt Studerus. Das sei wohl eher auf ein Bauchgefühl zurückzuführen. "Denn es gibt keine echten Gründe, die gegen die Nutzung der Cloud sprechen würden", sagt der CEO.

Wie Ivan Bütler im Auftrag des SRF einen Weihnachtsbaum hackt

Die erste Keynote des Tages hielt Ivan Bütler, CEO von Compass Security. Bütler hatte für die SRF-Sendung Blackout Anfang 2017 live im Fernsehen den Energieversorger EBL gehackt, die Genossenschaft Elektra Baselland. Das Ziel: Die Weihnachtsbeleuchtung abzuschalten.

Ivan Bütler, CEO von Compass Security. (Source: Netzmedien)

Ein paar Sachen waren zwar im Vorfeld abgemacht – die EBL war involviert und wusste davon. Dennoch handelte es sich im Wesentlichen um einen realen Angriff. In seinem Vortrag erklärte Bütler, wie die Attacke ablief.

In einem ersten Schritt sammelte er die nötigen Informationen. Diese fand er relativ leicht, da die EBL im Internet gut präsent ist: eine moderne Website, Blogs, einen gepflegten Facebook-Auftritt. In den Geschäftsberichten auf der Website fand Bütler etwa die Handynummer eines Geschäftsleitungsmitglieds.

Der Samichlaus-Angriff

Der erste Angriffsversuch erfolgte über eine gefälschte Bewerbung auf einem präparierten USB-Stick. Eine Methode, die oft zum Ziel führt. In diesem Fall allerdings nicht. Also versuchte Bütler es erneut, diesmal per E-Mail. Im Anhang war eine infizierte Word-Datei. Allerdings war auch dies nicht von Erfolg gekrönt. Also griff er auf härtere Methoden zurück: den Samichlaus-Angriff, wie er es nannte.

Zwei Mitarbeiter Bütlers verkleideten sich als Samichlaus und Schmutzli und liefen beim Firmensitz von EBL hinein. Dort erregten sie viel Aufmerksamkeit. Sogar der Chef von EBL kam, um zu sehen, was los war. Und der liess sich nicht übertölpeln. Ihm war sofort klar, dass dies wohl etwas mit der SRF-Sendung zu tun haben müsste.

Was ihm – und auch keiner anderen Person auffiel: Hinter Chlaus und Schmutzli schlich sich ein dritter Compass-Mitarbeiter in das Firmengebäude hinein – getarnt als Druckertechniker. Der Empfang, abgelenkt von den Kostümierten, bemerkte ihn nicht.

So lief der Eindringling ungehindert herum, bis er einen leeren Meeting-Raum mit PC fand. Dieser war zwar nur für Gäste bestimmt und mit minimalen Rechten bestückt. Aber auch der Gast-PC war Teil des Active Directory. Oder anders gesagt: Bütler hatte sein Einfallstor gefunden.

"Wer die Kontrolle über das Active Directory hat, hat in der Regel die volle Kontrolle darüber, was auf den Firmen-Laptops läuft", sagte Bütler. Eine kurze Suche und ein paar Powershell-Kommandos später war Bütler im Besitz des Passworts eines Enterprise-Administrators.

Noch eine Hürde

Das Passwort war zwar verschlüsselt, doch netterweise bietet Microsoft den Key zur Entschlüsselung online in seiner Dokumentation an. Nach ein wenig Trial und Error kannte Bütler das Passwort. Mit dieser neuen Macht, machte sich Bütler an den Laptop eines EBL-Mitarbeiters zu schaffen, der Fernwartungen ausübt. Ein Trojaner war alles, was er brauchte, um selber auch auf das EBL-Fernwartungs-Tool zugreifen zu können.

Tefo-Moderatorin Aileen Zumstein. (Source: Netzmedien)

Die letzte Hürde: Um die Einstellungen zu ändern, musste er noch ein Passwort eingeben. Da er als Administrator nun Software installieren konnte, war dies jedoch kein grosses Problem. Er installierte einen Keylogger auf den Laptop, und rief den Mitarbeiter kurzerhand an und meldete eine Störung. Dabei nutzte er ein Tool, das dem Angerufenen vorgaukelte, der Anruf käme vom EBL-Kundendienst.

Et voilà: Der Mitarbeiter tippte sein Passwort ein, der Keylogger merkte sich jeden Tastenanschlag und Bütler las mit. "Dann hatte ich alles zusammen", sagte Bütler. Er kippte einen Schalter im Fernwartungs-Tool und dann war der Weihnachtsbaum dunkel.

Keynote, Unterhaltung und Award-Vergabe stehen noch bevor

Das Tefo läuft noch den ganzen Tag weiter. Zu den weiteren Highlights gehören etwa noch die Keynote von Jürg Leuthold, Professor am Institute of Electromagnetic Fields der ETH Zürich. Er wird über die Kommunikation der Zukunft referieren.

Der Stimmenimitator David Bröckelmann am Tefo17. (Source: Netzmedien)

Schauspieler David Bröckelmann wird am Nachmittag noch für Unterhaltung sorgen. Gemäss Agenda soll der Imitator "die Promis ans Tefo bringen". Der Abschluss des Anlasses wird wie gewohnt die Verleihung des Studerus-Projekt-Awards. Nomiert dafür sind die Unternehmen Domatech, Mobilcom Systems und Valentin Tools.

Wer den Award mit nach Hause nimmt, lesen Sie an dieser Stelle.

https://www.it-markt.ch/news/2017-11-23/anatomie-eines-live-hacks-am-tefo-17