«Die heutigen Computersysteme sind viel zu komplex und zu offen vorkonfiguriert»

Die Cybercrime-Szene professionalisiert sich. Das Risiko, Opfer einer Attacke zu werden, wird grösser. Dabei könnten laut Thomas Dübendorfer gerade auch Soft- und Hardwareanbieter mit scheinbar einfachen Rezepten viel dazu beitragen, dass die Nutzer ruhiger schlafen können. Interview: Simon Zaugg, René Mosbacher

ZUR PERSON

Thomas Dübendorfer

WERDEGANG

Thomas Dübendorfer arbeitet als Software Engineer und Tech Lead im Bereich IT-Sicherheit bei Google in Zürich. Er erhielt bereits drei der begehrten Google OC Awards für seine technischen Beiträge zur Sicherheit von Googles Online-Werbesystem und zu Googles Cloud-Computing-Infrastruktur. Er ist Präsident der Information Security Society Switzerland ISSS und als CISSP Security Professional zertifiziert. Er hat das höhere Lehramt absolviert und unterrichtet als Dozent für Netzwerksicherheit an der ETH Zürich. Er hat einen Doktortitel (PhD) sowie den Master of Science in Informatik mit Auszeichnung der ETH Zürich.

STICHWORTE

Was können Sie jederzeit empfehlen?
Überprüfen Sie regelmässig, dass Sie alle Sicherheits-Updates installiert haben und machen Sie ein Back-up Ihrer wichtigen Daten.

Worüber haben Sie kürzlich gelacht?
Über den Youtube-Video mit der Katze, die den kläffenden Hund erst anbellt und dann wieder miaut.

Was hat Sie zuletzt richtig geärgert?
Dass es in meinen Sommerferien Mitte Juli im Entlebuch die ganze Woche geregnet hat und das Brienzer Rothorn sogar eingeschneit wurde.

Was machen Sie heute in zehn Jahren?
Mich mit einer interessanten Herausforderung beschäftigen und mit anderen zusammen eine überzeugende Lösung entwickeln.

Herr Dübendorfer, welche Cyberattacke hat Sie in diesem Jahr bisher am meisten überrascht?
Was mich betroffen macht, ist die Grössenordnung. Es ist heute immer noch möglich, trotz Antivirenprogrammen Millionen von Computern zu infizieren. Das zeigte sich auch bei den kürzlich durch Google eingeblendeten Warnungen, die dem Sucher mitteilen, wenn sein Computer mit Malware infiziert sein könnte.

Ist das so, weil die Nutzer ihre Virenschutz-Updates verschlafen?
Nein, diese Malware wurde von den gängigen Antivirenprogrammen bisher gar nicht erkannt. Erkannt wird diese von Google dann, wenn der Nutzer seine Suchanfrage startet. Dieser Warnmechanismus ist neu, denn bisher wurden Nutzer bei Suchanfragen nur vor infizierten Websites gewarnt, die dieser besuchen wollte.

Was sind aus Ihrer Sicht denn die Haupttrends der letzten zwei Jahre?
Die Art der Attacken hat sich insgesamt nicht gross verändert. Doch die Professionalisierung der Cyberkriminellen hat enorm zugenommen. Das zeigt sich an der verstärkten Arbeitsteilung. Zudem steigt die Anzahl der Anbieter von Malware laufend. Ironie der Sache ist hier, dass diese oft Garantien für die Nichterkennung durch Antivirenprogramme abgeben. Dann gewinnen einschlägige Foren, in denen Nutzer Angriffsziele diskutieren und Schwachstellen offenlegen, an Zulauf. Letztlich gibt es auch immer mehr Aktivisten, die beispielsweise Distributed-Denial-of-Service(DDoS)-Attacken fahren.

Sie haben die Arbeitsteilung angesprochen. Haben Sie ein konkretes Beispiel dazu?
Es gibt Leute, die Construction Kits für Botnets bereitstellen. Über weitere Akteure aus dem Untergrund kann man Computer infizieren lassen. Am Ende muss dann derjenige, der die Tat ausführen will, von der Sache nur wenig verstehen.

Warum ist – systemisch gesehen – unsere IT heute so verletzlich?
Die heutigen Computersysteme sind viel zu komplex und zu offen vorkonfiguriert, als dass ein ungeschulter Benutzer die Systemsicherheit gewährleisten könnte. Integrierte, wartungsfreie Sicherheitsmechanismen und reduzierte Komplexität bei der Schnittstelle zum Benutzer sollten vermehrt beim Design zukünftiger Systeme berücksichtigt werden.

Das heisst, dass beispielsweise der Update-Mechanismus deutlich vereinfacht werden müsste?
Wenn nicht jeder Softwarehersteller seinen eigenen Update-Mechanismus verwenden, sondern für alle Windows-Programme ein einziger Update-Mechanismus existieren würde, wäre das Patchen wesentlich einfacher und bekannte Schwachstellen deutlich schneller behoben. Klar ist: Wie die Sicherheit im Detail zustande kommt, interessiert den Nutzer in der Regel nicht.

Können Sie das etwas näher erläutern?
Wenn ich heute E-Banking mache, kann ich im Hintergrund gleichzeitig Software installieren und unzählige Programme laufen lassen. Das wäre aber eigentlich gar nicht nötig. In dem Moment möchte ich nur auf einer Website eines Anbieters meine Zahlungen tätigen – und dabei davon ausgehen können, dass meine Sicherheit gewährleistet ist. Sichere Alternativen, wie das Booten von einer CD-ROM aus, sind dagegen alles andere als benutzerfreundlich, denn das dauert lange und der Nutzer muss ein neues Verhalten lernen.

An was liegt es denn, dass nicht hart daran gearbeitet wird, diese Komplexität zu verringern?
Sicherheit ist heute noch kein wirkliches Verkaufsargument. Die Leute schreien beispielsweise eher nach neuen Features in Webbrowsern und Smartphones. Und wenn ein Anbieter sagt, dass sein Gerät genau das Gleiche kann wie ein anderes, aber sicherer ist, wird es deswegen nicht unbedingt häufiger gekauft.

Das heisst dann aber auch, dass es illusorisch ist, die immer komplexer werdenden Systeme sicherheitstechnisch in den Griff zu bekommen.
Solange man mit dem System alles machen können will, ist das illusorisch. Früher hatte

Thomas Dübendorfer hat wesentlich dazu beigetragen, dass die Koordinationsplattform der IT-Sicherheitsverbände Swisssecurity.org zustande kommt.

«Wenn nicht jeder Softwarehersteller seinen eigenen Update-Mechanismus verwenden, sondern für alle Windows-Programme ein einziger Update-Mechanismus existieren würde, wäre das Patchen wesentlich einfacher und bekannte Schwachstellen deutlich schneller behoben.»

man das Konzept der Thin-Clients, wo auf dem Computer des Endbenutzers nur ganz wenig Software installiert war. Die Komplexität war bei den Mainframes oder auf Servern. Heute sprechen wir von Cloud Computing mit dem Webbrowser als Thin-Client. Möglicherweise geht es also wieder in eine ähnliche Richtung.

Dann könnte die Cloud zum Heilsbringer werden?

Cloud Computing ist das Commodity-Outsourcing von Rechenzentren und deshalb als Modell nicht prinzipiell neu. Mit dem Unterschied, dass es bei konventionellen Outsourcing-Projekten in vielen Fällen um Millionenbeträge geht. Dagegen können Kunden bei der Cloud zu wesentlich kleineren Beträgen Leistungen beziehen. Der sicherheitstechnische Vorteil ist hier, dass Cloud-Dienste-Anbieter bei Problemen an der Quelle eingreifen und ein sauberes Patch-Management betreiben können. Beim Kunden läuft dann in der Regel nur der Webbrowser. Wenn dieser regelmässige Updates macht, dann ist das sicherer, als ein ganzes Serversystem ohne eigene Sicherheitsleute selbst zu betreiben.

Oder der Kunde muss einen externen Dienstleister beiziehen.

In vielen Fällen geschieht dies aber gar nicht oder viel zu spät. Besonders gravierend ist das Problem heute bei SCADA-Systemen, die bei der Steuerung von Industrieanlagen zum Einsatz kommen. Viele Systeme, die heute im Einsatz sind, wurden gar nicht konzipiert, um ans Internet angeschlossen zu werden und laufen deshalb auch ohne Virenschutz. Das Einspielen von Updates muss manuell vor Ort geschehen, was langsam und aufwendig ist und daher oft nicht gemacht wird. Die Betreiber müssten die Systeme eigentlich komplett erneuern, um auch sicherheitstechnisch auf dem neusten Stand zu bleiben. Das ist aber teuer.

Auch Social Media ist derzeit ein heiss diskutiertes Sicherheitsthema.

Ein wichtiger Punkt ist die Vertrauenswürdigkeit von Informationen, die über Social Media verbreitet werden. Dabei geht oft vergessen, dass die Leute nur über ein Bild und den Namen identifiziert sind. Es gibt keinen starken Authentisierungsmechanismus in diesen Netzwerken. Die Leute haben heute dennoch ein grosses Vertrauen. Doch nicht selten kommt es auch zu Missbräuchen. Zum Beispiel bei Falschmeldungen, bei denen man nicht weiss, wer dahintersteckt. Via gehackten Twitter-Account wurde auch schon der Tod von Präsident Obama verkündet.

Dann ist es im Moment auch weniger ein Sicherheits-, sondern eher ein Vertrauensproblem?

Das Problem ist, dass die Systeme keine Verifizierung zulassen. Man weiss nicht, ob die Person, die hinter einem Profil steckt, echt ist. Es bleibt dann nichts anderes übrig, als zu vergleichen, ob das Handeln der Person im «echten» Leben und im virtuellen Leben übereinstimmen. Und auch dann hat man keine Garantie, dass nicht doch auf einmal jemand den Account hackt. Ein One-Time-Token beim Log-in würde das Ganze wieder verkomplizieren. Am besten wäre ein Mechanismus, den man als Benutzer gar nicht bemerkt. Eine Möglichkeit wäre, zu überprüfen, ob die Person auch tatsächlich am Computer sitzt. Das könnte durch Gesichtserkennung via Videokamera geschehen. Genau da haben wir aber ein Datenschutzproblem. Dienstleister, die beispielsweise über Social Media Kunden beraten, würden den Aufwand mit den One-Time-Tokens wohl gerne in Kauf nehmen. Sie wollen auf keinen Fall, dass jemand ihren Ruf schädigen kann.

«Viele ISSS-Mitglieder haben Angst, dass ihre Computer infiziert sein könnten, ohne dass sie es bisher merkten.»

Wie attraktiv ist die Schweiz für Internetkriminelle, um von hier aus zu operieren?
Was die Gesetzeslage angeht, ist die Schweiz gut aufgestellt. Zudem nimmt die Polizei die Lage ernst. Auch die Zusammenarbeit zwischen den Telekomprovidern und den Behörden funktioniert gut. Die Chance ist gross, dass Internetkriminelle, die längere Zeit von hier aus operieren, auffliegen.

Und die Schweiz als Angriffsziel?
Man muss sich immer fragen, wo es was zu holen gibt. Und da ist die Schweiz sicher interessant. Es gibt hier viele Firmen mit interessanten Daten – Banken, Versicherungen, aber auch Pharmaunternehmen. Dann ist die Gesellschaft auch recht wohlhabend. Die Gefahr ist sicher nicht zu unterschätzen.

Auf der anderen Seite sind die Sicherheitsstandards hier höher als in anderen Ländern. Ein Angriff «lohnt» sich dann im Endeffekt häufig nicht mehr …
Das ist beispielsweise beim E-Banking so. In der Schweiz haben wir neben Benutzernamen und Passwort noch ein drittes Sicherheitsmerkmal. In den USA fordern viele Banken nur Benutzernamen und Passwort beim Login. Diese bieten die Sicherheit nicht primär durch starke Authentisierung, sondern indem sie – wie die Kreditkartenindustrie – das Kundenverhalten analysieren und schauen, ob eine Transaktion zum normalen Verhalten des Kunden passt.

Bleiben wir in der Schweiz und kommen zu der Verbandslandschaft. Vor kurzem wurde die Plattform Swisssecurity.org ins Leben gerufen. Wie ist es dazu gekommen?
In der Schweizer IT-Verbandslandschaft gibt es eine grosse Zersplitterung, im Speziellen auch im Bereich Security. Es gibt mehr als ein Dutzend Vereine, die sich mit dem Thema beschäftigen. Normalerweise ist niemand in mehr als zwei Vereinen tätig. Viele Personen mit ähnlichen Sichtweisen und Problemen lernen sich so gar nicht erst kennen.

Und dann sind Sie aktiv geworden?
Ursprünglich habe ich, um den Austausch zwischen den Vereinen zu fördern, die Präsidenten von verschiedenen Vereinen zu ISSS in den Vorstand geholt. Der erhoffte Informationsfluss unter den Vereinen liess aber zu wünschen übrig. Die Idee zu Swisssecurity.org ist dann in Gesprächen mit anderen Vereinspräsidenten entstanden – insbesondere auch mit Pascal Kocher von DEFCON Switzerland und Sven Vetsch vom OWASP Switzerland Local Chapter.

Was bringt denn die Plattform konkret?
Die Plattform Swisssecurity.org basiert auf Google Apps, und die angeschlossenen Vereine können mittels Mailinglisten, Chats, Videokonferenzen und Onlinedokumenten Informationen untereinander austauschen. Besonders wichtig ist auch der Eventkalender. Diesbezüglich haben wir auch schon Anfragen von Firmen bekommen – da sind wir aber noch zurückhaltend. Hinter der Plattform steckt zudem keine rechtliche Struktur, Swisssecurity.org ist derzeit kein Verein.

Wenn man nach Fragen sucht, die Ihren Verband ISSS derzeit beschäftigen, dann stösst man auf Themen wie die Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF. Was können Sie dazu sagen?
Die Vernehmlassung zu VÜPF ist brandaktuell. Ende Juli gaben wir dazu auch eine Stellungnahme ab. Das Problem ist Folgendes: Das revidierte Bundesgesetz BÜPF ist im Parlament gescheitert, jetzt versucht man es mit einer neuen Verordnung. Diese soll eine Echtzeitüberwachung des Internets ermöglichen – quasi durch die Hintertür. Das ist rechtsstaatlich bedenklich, denn die gesetzlichen Grundlagen sind ja nicht da. ICTswitzerland steht im Übrigen hinter unserer Stellungnahme.

Sie sind seit 2007 Präsident von ISSS. Welches waren Ihre Meilensteine?
Die Mitgliederanzahl haben wir auf mittlerweile über 900 vergrössern können. Dann sind die Special Interest Groups – die sogenannten SIGs – heute sicher aktiver als bei meinem Amtsantritt. Es gibt zudem heute mehr Anlässe. Zu guter Letzt ist der Vorstand heute jünger und nicht mehr eine reine Männergruppe. Die Rechtsanwältin und heutige Vizepräsidentin Ursula Widmer wird voraussichtlich nächstes Jahr meine Nachfolge antreten.

Gibt es denn eine speziell weibliche Sicht auf IT-Security?
Eine Durchmischung bringt in jedem Fall etwas. Das haben wir auch in Diskussionen gemerkt, dass Frauen andere Aspekte einbringen. Aber beispielsweise zu sagen, dass die Männer stets technischere Sichtweisen und die Frauen eher gesamtgesellschaftlichere Aspekte eingebracht haben, wäre verkürzt.

Was sind eigentlich die grössten Sorgen der Mitglieder Ihres Verbands?
Malware und insbesondere Trojaner sind ein grosses Problem. In dem Zusammenhang wird oft das Schlagwort Advanced Persistent Threat genannt. Viele Mitglieder haben Angst, dass ihre Computer infiziert sein könnten, ohne dass sie es bisher merkten. Das Kernproblem ist, dass Malware heute personalisiert ist. Das heisst, dass jeder Infizierte eine leicht veränderte Version erhält. Das erschwert die Erkennung mit Signaturen wesentlich.

Was tun Antivirenprogramme-Hersteller dagegen?
Es könnte zu einem Paradigmenwechsel kommen. Das heisst, dass man vom Blacklist-Prinzip abrückt und dafür Whitelists macht. Das Antivirenprogramm erkennt dann beispielsweise, ob die Software von einem vertrauenswürdigen Hersteller kommt. Dann kann der Nutzer nur noch Programme ausführen, die auf einer Whitelist sind. Es ist klar: Das Blacklist-Prinzip, das nur als bösartig erkannte Software blockiert, funktioniert heute nur noch sehr schlecht. <

ZUM VERBAND

ISSS

Die Information Security Society Switzerland ISSS wurde 1993 als Verein (damals «FGSec») gegründet. Sie ist der aktivste schweizerische Information-Security-Verein und vernetzt gegen 900 Security Professionals, darunter über 100 Firmen. Sie befasset sich in Theorie und Praxis mit technischen und juristischen sicherheitsrelevanten Aspekten der Informationsgesellschaft. Die ISSS bietet Special Interest Groups zu aktuellen Themen der Informationssicherheit, Security-Veranstaltungen, einen Newsletter, zahlreiche Member-Benefits wie 15 Prozent Rabatt auf über 100 Security-Veranstaltungen und -kursen pro Jahr. Sie setzt sich konsequent ein für den Informationsaustausch von Information Security Professionals untereinander und die nachhaltige Berücksichtigung der Sicherheitsaspekte bei Architekturen, Konzepten und Systemen. Als unabhängiger Fachverein kommuniziert ISSS offen und informiert neutral. Eine Mitgliedschaft gibt es ab 20 Franken pro Jahr. Der aktuelle Veranstaltungskalender und News werden auf www.isss.ch publiziert.