News (http://www.eco.de/news) | 15.09.2014

„Einen Euro ausgeben, um Schaden von 100 Euro abzuwenden“ (http://www.eco.de/2014/news/einen-euro-ausgeben-um-schaden-von-100-euro-abzuwenden.html)

IT-Kriminelle sind darauf angewiesen, Sicherheitslücken in Software und Hardware auszunutzen, für die es noch keinen Schutz gibt – oder von denen die Öffentlichkeit noch nicht einmal Kenntnis besitzt. Dr. Stefan Frei, Dozent an der ETH Zürich, forscht zu der Frage, ob und in welchem Umfang Unternehmen und Behörden selbst brisante Informationen erwerben sollen – welche Folgen das für IT-Kriminalität als Geschäftsmodell hat und ob sich dadurch die durch Sicherheitsrisiken verursachten Kosten reduzieren lassen.

Herr Dr. Frei, welche Gefahren im Zusammenhang mit unserer IT werden gerne übersehen?

Wie sich immer wieder zeigt, wird Software oft viel länger verwendet als bei der Implementierung geplant. Windows XP ist ein schönes Beispiel. Außerdem durchdringt Software immer mehr Bereiche unserer Gesellschaft und wird oft nicht als solche erkannt, beispielsweise werden Kopierer oder Drucker typischerweise nicht als Computer erkannt, die ihre eigenen Schwachstellen haben – und bleiben entsprechend ungeschützt. Die rasant voranschreitende Vernetzung, das „Internet der Dinge“, lässt Software zudem vermehrt in Geräten mit Lebenszyklen weitab von dem, was wir uns aus der PC-Welt gewohnt sind, zum Einsatz kommen. Aus diesen Gründen sehe ich keine Beruhigung an der Gefährdungsfront.

Wir haben uns längst damit abgefunden, dass Cyberkriminalität ein lukratives Geschäft ist. Bei der Bekämpfung dieser Art von Kriminalität schlagen Sie Unternehmen vor, Daten zu neuen Schwachstellen käuflich zu erwerben und so Kriminelle aus dem Geschäft zu drängen. Wie haben wir uns das konkret vorzustellen?

Schwachstellen in den falschen Händen stellen eine Gefährdung für alle privaten wie auch geschäftlichen Softwarenutzer dar. Derzeit verlassen wir uns größtenteils darauf, dass der Entdecker einer Schwachstelle diese dem Hersteller meldet, und mit der Publikation wartet bis endlich ein Patch verfügbar ist. Der Softwarehersteller dankt dies in der Regel aber lediglich mit einem T-Shirt und einer Danksagung im Patch-Advisory. Auf der anderen Seite hat sich in den letzten Jahren ein lukrativer Schwarzmarkt für Schwachstellen und Exploits entwickelt. Für entsprechende Informationen werden durchaus 100.000 Dollar oder mehr bezahlt und das nicht nur von Kriminellen, sondern auch von Regierungsstellen.

-
-
-
-
-
-
-
-
-

Nächste eco Events

24.09.2014 | Brühl bei Köln
Internet Security Days 2014
(http://www.eco.de/2014/veranstaltungen/int
security-days-2014.html)

30.09.2014 | Berlin
Kompetenzgruppe Recht & Regulierung
(http://www.eco.de/2014/veranstaltungen/kc
recht-regulierung-2.html)

01.10.2014 | Berlin
eco Zukunftsdialog - Neuausrichtung der Internetverwaltung
(http://inetgov.eco.de/2014/events/eco-zukunftsdialog-neuausrichtung-der-internetverwaltung.html)

08.10.2014 | Nürnberg
Das perfekte Rechenzentrum – sicher von Anfang an!
(http://datacenter.eco.de/2014/events/das-perfekte-rechenzentrum-sicher-von-anfang-an.html)

Diese Entwicklung kann mit den bisherigen Ansätzen nicht gestoppt werden. Würden Softwarehersteller, Interessengruppen wie etwa die Finanz- oder Pharmabranche oder auch internationale Organisation wie die EU oder die Vereinten Nationen als Käufer auftreten und angemessene Preise bezahlen, hätten die Entdecker von Schwachstellen endlich eine Alternative. Mehr Schwachstellen würden kontrolliert gepatcht und dadurch stiegen die Kosten für Cyberkriminelle. Viele Angriffsszenarien würden sich schlicht nicht mehr lohnen. Unsere Untersuchungen (http://www.techzoom.net/papers/nss_international_vulnerability_purchase_program_lvpp_2013.pdf) zeigen, dass die Kosten eines solchen Programms im Vergleich zum Schaden, der abgewendet wird, sehr klein sind. Es macht wirtschaftlich Sinn, einen Euro auszugeben, um einen Schaden von 100 Euro abzuwenden.

Wie funktioniert ein solcher offener Handel mit Schwachstellen und in welchem Umfang wird er schon heute praktiziert?

(http://isd.eco.de/de/registrieren/)Es gibt verschiedene Arten von Programmen, welche Softwareschwachstellen („Bug Bounty Program“) aufkaufen. Zwei bekannte Anbieter von Sicherheitssoftware und Diensten betreiben seit zehn Jahren Aufkaufprogramme. Mit diesen Informationen erhalten sie einen Vorsprung, um ihre Kunden zu schützen, bis der Hersteller, den sie informieren, einen Patch bereitstellt. Daneben gibt es Wettbewerbe von Sicherheitsfirmen, bei denen Teams, welche eine vorgegebene Konfiguration erfolgreich hacken, mit namhaften Preisen für die verwendete Schwachstelle belohnt werden.

In den letzten Jahren sind Firmen wie BugCrowd entstanden, welche für Softwarehersteller ein Bug Bounty Program betreiben. Immer mehr Softwarehersteller bieten eigene Bug Bounty Programme an, um Schwachstellen in ihren eigenen Produkten aufzukaufen. Diese Programme bieten typischerweise erheblich weniger Geld, als im Untergrund für Schwachstellen bezahlt wird. Dennoch ist das Konzept, Schwachstellen aufzukaufen, um die Sicherheit als Benutzer oder Hersteller zu erhöhen, ist mittlerweile erprobt und etabliert. Es setzt sich immer weiter durch.

Aus anderen Bereichen der Verbrechensbekämpfung wissen wir: Wenn Kriminellen ein Geschäft entzogen wird, verlagern sie sich auf das nächste. Was könnte das für die IT-Landschaft bedeuten?

In unserer Gesellschaft wird mit großer Geschwindigkeit alles Mögliche und Unmögliche vernetzt und neue Sensoren speichern umfangreiche Daten über alle Aspekte unseres Lebens. Wir bauen ein komplexes System ungeahnten Ausmaßes. Diese Entwicklung bietet enorme Möglichkeiten, jedoch auch viele neue Missbrauchsszenarien und Betätigungsfelder für Kriminelle. Zum Beispiel verschlüsseln Kriminelle heute infizierte PCs und der Benutzer kann sich danach für ein paar hundert Dollar den Zugang zu seinen Daten wieder erkaufen. In Zukunft wird vielleicht einem Haus oder einer Siedlung Strom oder Wasser abgeschaltet, das Auto blockiert und so weiter.

Dr. Stefan Frei spricht zum Thema „The Known Unknowns in Cyber Security & Outbidding Cyber Criminals“ am 24. September 2014 (http://isd.eco.de/de/agenda-2/agenda-2014-mittwoch/) bei den Internet Security Days (http://isd.eco.de/).

(http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html)

14.10.2014 | Berlin
Notfallmanagement für Ihr Rechenzentrum - Berlin
(http://datacenter.eco.de/2014/events/notfall fuer-ihr-rechenzentrum.html)

eco Politikbrief

Politikbrief

Ausgabe 2.2014: Europa entdeckt das Internet
(http://www.eco.de/wp-content/blogs.dir/eco_politbrief2_2014_web

eco Trend-Surfing

Diese Woche: „Strype: Digitales Siegel sichert Eigentum“
(http://www.eco.de/trend-surfing.html)