Tageblatt
Donnerstag, 1. September 2022 • Nr. 202

Die Lautlosen der Post

INTERNET Mit offensiver Sicherheit gegen Hacker

Claude Molinaro

Bei der Post gibt es seit 2019 ein etwa 50 Personen starkes Cyberforce-Team, das jeden Aspekt der Internet-Sicherheit abdeckt. Zum Team gehören neun Männer und Frauen, die die Sache wesentlich offensiver angehen und Firmenkunden mit den gleichen Mitteln helfen, wie Cyber-Kriminelle sie nutzen.

Fotos: Editpress/Tania Feller

Jean-Marie Bourbon und sein Team treten kriminellen Hackern mit deren eigenen Mitteln entgegen

„Man muss bedenken, dass das Internet nicht mit der Idee von Sicherheit konzipiert wurde", sagt Jean-Marie Bourbon, Leiter der „Offensive Security Services" bei der Post. Praktisch jede Firma nutze heute das Internet; schon allein der Kontakt mit den Geschäftspartnern im Web könnte eine potenzielle Gefahr darstellen. Das Thema Internetsicherheit ist sehr vielfältig; dementsprechend vielfältig müssen auch die Antworten der Sicherheitsexperten sein. Innerhalb der Cyberforce-Abteilung der Post gibt es das „Security Operations Center", welches die Netzwerke der Kunden überwacht und unerlaubte „Einbrüche" aufzeichnet. Dann gibt es ein Team, das die Sicherheitsvorfälle verwaltet und ständig neue Bedrohungen analysiert.

Und dann gibt es die Abteilung „Offensive Security Services", die eigentlich genau das Gleiche tut wie die bösen Jungs und Mädchen im Internet auch, nur eben im Interesse der Postkunden. Deshalb werden sie auch manchmal „ethical hacker" oder „white hat hacker" genannt (im Gegensatz zu den kriminellen „black hat hacker").

Im Film „Sneakers – Die Lautlosen" aus dem Jahr 1992 decken Robert Redford und seine Freunde Schwachstellen in Sicherheitssystemen von Banken gegen Bezahlung auf. Auch wenn es ein Hollywoodfilm ist, die Arbeit der „Offensive Security" kommt jener der Filmhelden in einigen Aspekten sehr nahe. Es sei eine Sache, auf dem Papier hohe Sicherheitsstandards vorweisen zu können, aber solange sie nicht unter reellen Gegebenheiten getestet seien, wisse man nicht, wie effizient sie sind, sagt Bourbon. Er und seine „Sneakers" testen im Auftrag von Großkunden die Sicherheit derer Systeme. Sie simulieren Angriffe, wie sie auch im reellen Leben stattfinden können.

Auch physische Angriffe

Und das geht manchmal über Phishing-Angriffe oder das unerlaubte Eindringen in ein Netzwerk hinaus. „Zur Aufgabe des Teams gehören auch physische Angriffe", erklärt Pierre Zimmer, beigeordneter Generaldirektor und „Chief Strategy Officer" der Post. „Dabei müssen sie z.B. versuchen, beim Kunden in den Raum einzudringen, wo die Server stehen. Als Beweis für einen erfolgreichen Versuch hinterlassen sie eine Botschaft im Stil von 'Wir waren hier'."

Bourbon zeigt uns ein Hilfsmittel seiner Arbeit: einen langen, gebogenen Draht. „Schauen Sie, ich zeige Ihnen etwas: In etlichen Gebäuden gibt es Türen, die sich nur mit Hilfe eines Sicherheitsausweises öffnen lassen, aber nur um *in* den geschützten Bereich zu gelangen, nicht aber, um herauszukommen. Mit diesem Kabel kann man unter der Tür hindurchgreifen, die Klinke greifen und die Tür von innen öffnen, und schon hat man ein Hindernis überwunden." Zu physischen Angriffen könne auch gehören, um drei Uhr morgens vor einem Gebäude eines Kunden zu beobachten, wie der Reinigungsdienst in das Firmengebäude kommt, um auch dieses Wissen eventuell auszunutzen, ergänzt Zimmer.

Kann man als Privatperson schon mit einigen wenigen Maßnahmen (s. Kasten) einiges in Sachen Computer-Sicherheit tun, stellt sich die Lage für Unternehmen anders dar. Die richtig bösen Jungs und Mädchen im Internet haben heute oft als organisierte Banden eher Firmen im Visier, da sich damit mehr Geld ergaunern lässt. Hacking ist ein Geschäftsmodell. Kriminelle Hacker verkaufen oft die erbeuteten Zugänge zu Netzwerken an ihre „Kunden" weiter.

Encevo kein Postkunde

Das kürzlich von Hackern angegriffene Unternehmen Encevo sei übrigens kein Postkunde in Sachen Internetsicherheit, sagt Pierre Zimmer auf Nachfrage. Auch sei die Post nach dem Angriff auf den Stromversorger nicht um Unterstützung gebeten worden.

Zur Arbeit der „guten" Hacker der Post gehören neben den erwähnten physischen Tests auch reine Computer-basierte Angriffe wie Phishing, welches, wie dem kürzlich veröffentlichten Quartalsbericht der „Cyberforce" der Post zu entnehmen ist, noch immer die beliebteste Angriffsmethode von kriminellen Hackern ist. Laut dem Bericht ist die Zahl an Cyberangriffen im zweiten Quartal um zehn Prozent im Vergleich zum Beginn des Jahres gesunken. „Die Anzahl der Phishing-Angriffe und ihr Anteil im Vergleich zu anderen Arten von Vorfällen lassen sich durch ihren Erfolg bei der Erreichung ihres Ziels erklären, ebenso wie durch die Leichtigkeit, mit der diese Art von Angriff durchgeführt werden kann", schreibt die Post.

„Die Zeiten, in denen Unternehmen eine oder zwei Personen hatten, die für die Netzsicherheit verantwortlich waren, sind längst vorbei", sagt Zimmer. „Der Bereich 'Cyber-Sicherheit' ist ein sehr weites Feld, und es gibt Spezialisten für alles." Hinzu komme, dass es stets Neues in dem Bereich gebe: Die kriminellen Hacker entwickeln ihre Methoden stets weiter und die Sicherheitsexperten müssen dabei mithalten. Da es deswegen keine festgeschriebene Methodologie bei ihrer Arbeit gebe, müsse man Einfallsreichtum beweisen. „Wir müssen kreativ sein", sagt Bourbon.

Das führe dazu, dass man bei der Post nicht nur darauf bedacht sei, Spezialisten einzustellen, sondern Leute, die von der Sache begeistert sind. „Wir wollen Experten, die Freude daran haben, zur Arbeit zu kommen, und vor allem auch Spaß daran haben, ständig hinzuzulernen", sagt Zimmer.

„Die Herausforderung ist aber nicht nur, gute Leute zu finden, sondern sie auch zu behalten", sagt Bourbon. Eine Aussage, die vor dem Hintergrund der Zahlen in dem Sektor leicht zu verstehen ist. Laut der „Cybersecurity Workforce Study" fehlten 2021 in Deutschland 68.000 Cybersicherheitsexperten, in Frankreich waren es 28.000. Zahlen über Luxemburg liefert die Studie nicht, man kann sich aber vorstellen, dass auch hierzulande Experten in dem Bereich gesucht sind. Dass das „Lycée Guillaume Kroll" in Esch/Alzette ein „Brevet de technicien supérieur en cybersécurité"-Studium anbietet, kommt wohl nicht von ungefähr.

Man wolle aber keine Leute, die nur einen achtstündigen Bürojob wollen. „Unsere Job-Interviews sind deshalb etwas unkonventionell und die Profile der Kandidaten manchmal ungewöhnlich", sagt Pierre Zimmer. Unter anderem muss ein Kandidat in einem Praxistest zeigen, was er draufhat.

Vom Bäcker zum Hacker

Ob der geeignete Kandidat über einen Hochschul-Abschluss in dem Bereich verfügt, sei aber zweitrangig. Der Weg zum Cyber-Security-Experten führe nicht gezwungenermaßen über ein klassisches Uni-Diplom. Das beste Beispiel dafür ist der Chef der offensiven Sicherheitsmannschaft selbst. Der 41-jährige Jean-Marie Bourbon war vor seiner Karriere als Internet-Sicherheitsexperte Bäcker in Nîmes. 2006 habe seine Frau ihn überzeugt, sie bräuchten einen Computer für ihr Geschäft – gesagt, getan. Doch nach einem Monat sei dieser bereits mit einem Schadprogramm infiziert gewesen. Da der zu Hilfe gerufene Computerspezialist ihm auch nicht genau sagen konnte, wie ein „Trojaner" funktioniere, habe er selber recherchiert. U.a. habe es ihn fasziniert, wie man auf Distanz einen Computer manipulieren kann. „Anstatt mir nach der Arbeit einen Mittagsschlaf zu gönnen, recherchierte und las ich über das Thema, knüpfte Kontakte zu Gleichgesinnten im Internet. Später nahm ich mit einer Mannschaft an internationalen Hackerwettstreiten teil; alles neben meinem Beruf als Bäcker."

Als er bereits ein Experte auf dem Gebiet der Cyber-Sicherheit war, formalisierte er sein Wissen mittels eines „baccalauréat professionnel" in Wartung von Computernetzwerken. Seit zwei Jahren arbeitet Bourbon nun bei der Post. Dass er für den Job von weit herkommt, ist nicht ungewöhnlich: Es sei schwierig, in dem Bereich gute Fachleute zu finden. In dem neunköpfigen Team der offensiven Sicherheit ist Englisch Hauptkommunikationssprache.

Es gebe eine Gemeinsamkeit zwischen seinem ehemaligen und jetzigen Beruf. „In beiden Fällen muss man von seiner Arbeit begeistert sein, um gute Resultate zu erreichen." Im Unterschied zu anderen IT-Experten sei er aber wohl vielleicht der einzige, der seinen Mitarbeitern selbstgebackene Croissants mitbringen könne.

Mehr PC-Sicherheit: zehn goldene Regeln

- Virenschutz benutzen
- Anwendungen auf dem neuesten Stand halten
- Backups anfertigen
- Mails sorgfältig prüfen
- Verdächtige Dateien testen (z.B. bei Virustotal)
- Sichere Passwörter nutzen
- Zwei-Faktor-Authentifizierung (2FA) nutzen
- Bildschirmsperren einrichten
- Vorsicht bei der Nutzung eines fremden WLANs
- Keine Programme von dubiosen Servern herunterladen

Ransomware: PC nicht ausschalten!

Eine unter Cyberkriminellen beliebte Methode zur Geldbeschaffung ist eine sogenannte „Ransomware". Es handelt sich dabei um Schadprogramme, die den Zugriff auf Daten und Computer einschränken oder ganz unterbinden. Für die Freigabe fordern die Täter ein Lösegeld (englisch: Ransom).
Die Experten geben dazu zwei Tipps:
Erstens, nicht auf die Forderungen der Täter eingehen, denn wenn sie einmal Geld erhielten, gebe es keine Gewissheit, dass die gleiche Schwachstelle nicht noch einmal ausgenutzt wird.
Zweitens soll man den PC oder das System bei einem solchen Vorfall nicht ausschalten; oft gebe es wichtige Hinweise auf die Täter