»OBSERVER«

Die Presse
Unabhängige Tageszeitung für Österreich
Wien, am 24.06.2016, 312x/Jahr, Seite: _
Druckauflage: 83 582, Größe: 62,53%, easyAPQ: _
Auftr.: 2263, Clip: 9860865, SB: Webster Vienna Private University

„Daten nie in der Cloud speichern“

Interview. Der US-amerikanische Internet-Sicherheitsexperte Thomas Johnson über die Schwachstellen in Netzwerken, neue Tricks von Hackern und über Cyber-Terroristen.

VON NORBERT RIEF

Die Presse: In den vergangenen Jahren wurde viele große Unternehmen – darunter Google, Yahoo, Microsoft – Opfer von Hackerattacken. Ist es heute nicht mehr eine Frage, ob, sondern nur noch wann ein Unternehmen gehackt wird?
Thomas Johnson: Ja. Es ist unglaublich, wie viele Angriffe es bereits auf viele verschiedene Unternehmen gegeben hat. Dafür müssen sich diese Firmen selbst Vorwürfe machen, weil sie viele Jahre nicht in die Sicherheit ihrer Systeme investiert haben.

Was waren die größten Schwachstelle im System, die die Angriffe möglich gemacht haben?
Hacker sind auf viele verschiedene Arten in die Systeme eingebrochen. Derzeit machen uns Advanced-Persistent-Threat(APT)-Angriffe die größten Sorgen. Hacker nehmen sich dafür sehr viel Zeit und betreiben großen Aufwand, um etwa das Privatleben des Firmenchefs oder leitenden Managers auszuspionieren. An sie schickt man dann gezielte, vermeintliche persönliche Mails. Sobald sie auf einen Link klicken oder ein Attachment öffnen, ist ihr System infiziert und die Hacker sind da.

So etwas muss man doch sofort bemerken!
Der neue Trick ist, Daten, die man aus einer Firma herausholt, zu verschlüsseln. So weiß ein Unternehmen nicht, welche Informationen oder welche Daten gestohlen wurden. Die Sicherheitssysteme schlagen nicht an.

Wie lang geht das, bevor es bemerkt wird?
Bei Angriffen durch Hacker des chinesischen Militärs haben wir gesehen, dass sie im Durchschnitt – noch einmal: im Durchschnitt – 243 Tage im System waren, bevor es aufgefallen ist. Das ist unglaublich. Wenn man fast ein Jahr Zeit hat, sich in einem System umzuschauen und Datenbanken zu erforschen, kann man enorm viel Schaden anrichten.

Thomas Johnson arbeitete unter anderem für das FBI und den Secret Service. [Akos Burg]

Was kann man dagegen tun?
Ich rate Firmen, nicht unbedingt alle Ressourcen darauf zu verwenden, Systeme vor Zugriffen von Hackern zu schützen. Das ist zwar wichtig, wird aber oft überschätzt. Irgendwann kommen die Hacker ins System, etwa dank Zero-Day-Attacks *(Lücken im System, die noch nie benutzt wurden, Anm.)*. Wichtiger ist es daher zu verhindern, dass Hacker, die einmal im System sind, Daten stehlen oder Schaden anrichten können.

Und wie verhindert man das?
Indem man viel Geld in die Hand nimmt. Man braucht entsprechend ausgebildetes Personal, und man muss die Bedrohung ernst nehmen. Man kämpft mittlerweile gegen organisierte Banden, die ihr Geld mit gezielten Hackerangriffen machen oder die ihre Dienste sogar im Internet anbieten.

Von den Kindern, die aus Langeweile Systeme hacken, ist man weit weg?
Früher war es so, da haben Kinder solche Sachen einfach aus Spaß gemacht. Heute ist alles viel organisierter und geplanter. Wir haben mit Freizeithackern angefangen, dann sind einzelne Kriminellen gekommen, danach die organisierte Kriminalität, die das Internet zum Geldverdienen entdeckt hat, und jetzt geht es um Industriespionage und Cyber-Terroristen.

Was war die schwerwiegendste Cyber-Attacke?
Nicht alle sind bekannt, weil manche Unternehmen die Angriffe aus Angst vor den Folgen nicht öffentlich machen. Einer der größten bekannten Angriffe war sicher der auf Target *(2013 griffen Hacker die US-Kaufhauskette an, sie hatten Zugriff auf 40 Millionen Kundendaten und auf jede einzelne Kasse in den Hunderten Filialen, Anm.)*. Wir hatten auch ein Krankenhaus in den USA, dessen Datenbank von Hackern verschlüsselt wurde. Sie konnten also auf keine Patientendaten mehr zugreifen. Sie zahlten den Hackern 750.000 Dollar, damit sie das System wieder frei geben und die Datenbank entschlüsseln.

Sie haben die Cyber-Terroristen erwähnt: In den 1990er-Jahren galt, dass man mit 15, 20 guten Hackern die Infrastruktur eines ganzen Landes lahmlegen kann. Ist das noch so?
Ein ganzes Land ausschalten geht wahrscheinlich nicht mehr, aber man kann sehr viel Schaden in einzelnen Bereichen anrichten. Man kann beispielsweise die Flugkontrolle ausschalten und so den Flugverkehr lahmlegen. Oder den Finanzbereich, wenn man die Hacker auf die Wall Street konzentriert. Unmöglich ist es nie, alle Systeme haben eine Schwachstelle.

Was sind denn bekannte Schwachstellen?
Viele Unternehmen schaffen sich ihre eigenen Angriffsflächen, etwa mit der BYOD-Politik *(Bring your own device, die Angestellten bringen beispielsweise ihre privaten Laptops in die Arbeit mit)*. In diesen Fällen muss man sich sehr genau überlegen, wie viel Zugang man den Mitarbeitern zum Netzwerk gibt. Das Gleiche gilt für Handys, das sind die neuen großen Gefahrenquellen. In vielen Militäreinrichtungen in den USA darf man beispielsweise kein privates Smartphone mitbringen, weil die Mobiltelefone einfach zu viel können und zu gefährlich sind.

Von den gelangweilten Hackerkids zu Cyber-Terroristen – was kommt als Nächstes? Wovor müssen wir uns in zehn Jahren schützen?
Der Schutz beginnt in der Schule mit der Ausbildung der Kinder. Sie haben heute unglaubliche Fähigkeiten, weil sie mit der Technologie aufwachsen. Für sie ist das völlig selbstverständlich. Ein Freund bat mich beispielsweise um Hilfe, weil die Kinder in seiner Nachbarschaft einen seltsamen Zeitvertreib hatten: Sie hackten sich in die Computer der anderen Kinder und löschten die Daten – nur waren es manchmal die Computer der Eltern. Die Kinder von heute können die Hacker der Zukunft sein – oder sie sind diejenigen, die uns vor Hackern schützen. Das ist alles eine Frage, welche Werte man ihnen vermittelt.

Weil wir so viel über die Sicherheit von Daten gesprochen haben: Speichern Sie Ihre privaten Daten in der Internet-Cloud, also beispielsweise auf Servern von Amazon oder Google?
Amazon ist gut, die haben in den vergangenen Jahren eine ziemlich gute Arbeit geleistet. Aber ich würde meine Daten nie in einer öffentlichen Cloud speichern.

ZUR PERSON

Thomas Johnson war Mitglied der Electronic Crime Task Force des US Secret Service. Er arbeitete auch für die amerikanische Bundespolizei FBI und war Berater einer Taskforce des kalifornischen Gerichts. Johnson schrieb mehrere Bücher, zuletzt „Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare“. Johnson hat für die Webster Vienna Private University einen Cybersecurity-Ausbildungsschwerpunkt entwickelt, der heuer im Herbst startet.