«Alle sind angreifbar»

IT-Sicherheit Am Ostschweizer Technologiesymposium hat der weltweit bekannte Ex-Hacker Gunnar Porada die Sicherheit von Computersystemen thematisiert. Spektakulär sind stets seine Live-Hacks wie etwa Angriffe auf Bankkonten oder Web-Applikationen.

Interview: Stefan Borkert

Gunnar Porada deckt Sicherheitslücken in Computersystemen auf. Bild: PD

Gunnar Porada, wann sind Sie das letzte Mal selbst gehackt worden?
Wir werden alle permanent gehackt. Denken Sie nur an die Regierungsangriffe weltweit. Hinzu kommen noch kriminelle Hacker, die auf eigene Faust oder organisiert handeln. Wobei die Trennung spätestens hinter der Landesgrenze bei staatlichen Hackern schwerfällt. Die Frage ist also nicht, wann oder ob ich gehackt werde, sondern, ob ich es merke. Und das bemerke ich sehr oft. Einzelheiten darüber zu veröffentlichen, wären aber kontraproduktiv für mich.

Was war Ihr grösster Hack, den Sie ohne strafrechtliche Konsequenzen mitteilen dürfen?
Da gibt es eine ganze Reihe, da wir ja dafür beauftragt werden, dies regelmässig zu tun. Wir haben sehr vieles gesehen und sehr viele Systeme erschreckend schnell unter Kontrolle gebracht. Als Jugendlicher habe ich angefangen mit kostenlosem Telefonieren, das sogenannte Blue-Boxing. Das haben zu der damaligen Zeit viele gemacht, auch Steve Jobs. Später haben wir aber auch noch die Frequenzfilter in den Leitungen hacken können, was zu jener Zeit meines Wissens noch kaum jemand geschafft hatte. Wir hatten schlagartig viele Freunde. Und dann haben wir noch den Master-Key der alten EC-Karten gehackt. Der hatte damals allerdings nur 56 Bit. Hinzu kamen viele andere Dinge, die zu jener Zeit noch nicht illegal waren. Überhaupt lege ich Wert darauf zu betonen, dass wir uns immer an Gesetze halten. An uns werden öfters Anfragen gestellt von Leuten, die Hacker für kriminelle Handlungen suchen. Das lehnen wir strikt ab.

Welche Barrieren, Firewalls haben Sie an Ihre Grenzen gebracht?
Die Ahnungslosigkeit vieler Entscheider, wenn sie gegen jeden Rat und Hinweis, selbst von den eigenen Mitarbeitern, wieder ein System durchpeitschen, von dem alle wissen, dass es einem bald um die Ohren fliegt.

Welchen Fehler würden Sie nie wieder machen?
Schwachstellen den Opfern melden und dann auch noch hoffen, dafür angemessen behandelt und entlohnt zu werden.

Wie sicher sind Ihre privaten Computer, Tablets, Smartphones?
Ich trenne Arbeitsgeräte, bei denen ich paranoid bin und mich um die Sicherheit kümmere. Und dann nutze ich auch Geräte, bei denen es egal ist. Ich behandle die Technik aber entsprechend und vermeide Schäden grundsätzlich schon im Vorfeld durch Datensparsamkeit.

Sie treten als Ex-Hacker auf, auch in den Olma-Hallen am Technologie-Symposium in St. Gallen. Wie wird man Ex-Hacker?
Der Begriff Hacker ist nicht definiert. Viele Personen glauben immer noch, dass alle Hacker böse sind. Das ist notabene definitiv falsch, weil es eine neutrale Bezeichnung ist. Also versuche ich, das mit dem Ex zu entschärfen. Gleichzeitig möchte ich aber aufzeigen, dass wir die Technik tatsächlich kennen und die Angreifer natürlich auch. Das ist notwendig, wenn Sie effektiv sein wollen bei der Abwehr von kriminellen Hackern.

> «An uns werden öfters Anfragen gestellt von Leuten, die Hacker für kriminelle Handlungen suchen. Das lehnen wir aber strikt ab.»
>
> **Gunnar Porada**
> Gründer Innosec GmbH, Weggis

Sie arbeiten mit Live-Hacks bei Ihren Vorträgen. Dabei kommt es schon mal zu Überweisungen in Millionenhöhe, allerdings nicht bei der echten Deutschen Bank. Verliert Ihre Argumentation dadurch nicht an Durchschlagskraft?
Es gibt natürlich Menschen, die es erst dann glauben, wenn es ihnen im realen Leben passiert ist. Ich versuche, die Leute abzuholen, zumindest diejenigen, die das Thema dann ernst nehmen, wenn sie sehen, wie ein Hack funktionieren könnte. Denn den anderen kann man oft hinterher auch nicht mehr helfen, weil es dann einfach zu spät ist. Beim Thema Onlinebanking oder Geld hören zumindest alle zu, und ein paar Teilnehmern öffnet es auch die Augen. Im Rahmen der Legalität versuche ich den Hack möglichst realitätsnah zu zeigen. Ausserdem möchte ich das Thema auch verständlich und anschaulich vermitteln.

Könnten Sie, Stand heute, ebenso leicht in das System einer realen Bank, etwa der St. Galler Kantonalbank eindringen?
Wir haben Kunden im Bankenumfeld, über die wir nicht im Detail sprechen dürfen und wollen. Aber wir hatten schon Fälle, in denen wir die Kontrolle der Server übernommen haben. Das ist keine Schande, denn die haben uns ja genau dazu engagiert, nämlich sie zu hacken. Und damit haben diese Unternehmen es richtig gemacht, denn sie erfahren von Lücken, bevor sie missbraucht werden und können sie dann schliessen.

Ist die Überwindung der Sicherheitssysteme einfacher bei Grossbanken oder kleineren Banken?
Das hängt davon ab, wie gut oder schlecht sie die Systeme abgesichert haben. Grosse Konzerne und auch Banken tendieren oft dazu, mit der Masse zu gehen, was im Sicherheitsumfeld nicht immer ratsam ist. Gleichzeitig haben sie auch eine grössere Angriffsfläche. Nehmen Sie Google als Beispiel. Ich habe Mitarbeiter, die sich bei denen eine goldene Nase verdient haben, weil Google für das Auffinden von Schwachstellen bezahlt, genannt Bug-Bounty. Das machen noch viele andere Unternehmen auch, zusätzlich zu weiteren Sicherheitsmassnahmen.

Welche Fehler machen speziell Unternehmen beim Systemschutz?
IT-Sicherheit sollte Chefsache sein. Diese aber zieren sich oft und sind überfordert. Chefs versuchen zu delegieren. Das geht dann oft so weit, bis die Sache ganz aus dem Unternehmen ausgelagert wird, beispielsweise in die Cloud. Dabei vergessen viele, dass, wenn der Schadensfall eintritt, dieser am heftigsten genau in der Chefetage aufschlägt. Ich denke, die Zukunft wird eine Art natürliche Selektion durchführen. Es werden Unternehmen überleben, die das Thema besser verstehen. Für eine Verbesserung wird das Thema an der Uni Liechtenstein neuerdings verstärkt in der Wirtschaftsinformatik aufgegriffen.

Ist die zunehmende Digitalisierung, autonomes Fahren und die Robotik nicht ein Einfallstor für böswillige Manipulationen?
Natürlich. Ich habe vor knapp 20 Jahren selber einen Robotershop betrieben. Meine damaligen Roboterbausätze stehen im weltweit grössten Computermuseum in Paderborn. Dort stehen sie, weil es im Endeffekt alles nur Computer sind, egal ob sie in Robotern stecken, in Autos, Ampeln, Telefonen oder einfach nur in Ihrem Fernseher. Alle sind angreifbar. Die Möglichkeiten nehmen auf beiden Seiten zu.

Hundertprozentigen Schutz gibt es nicht. Trotzdem ist die Wirtschaft, sind wir, abhängig vom digitalen Fortschritt. Wird es eine Zurück-auf-die-Bäume-Bewegung geben?
Ein Zurück wird es nicht geben können, zumindest nicht freiwillig. Das braucht es aber auch nicht, wenn wir das Gleichgewicht zwischen Sicherheit und Fortschritt im Auge behalten.

Gibt es eine Zahl, wie hoch der Nachholbedarf in puncto digitaler Sicherheit bei Schweizer KMU ist?
Die Definition KMU gibt es bei mir nicht. Zum einen finde ich es vermessen, einem Unternehmer zu sagen, dass seine Firma klein ist, obwohl sie für den Gründer oder Chef sicher das Grösste ist. Dazu zähle ich auch meine Firma. Zum anderen haben wir Kunden, die nur eine Handvoll Computer haben, aber mit Milliarden Beträgen arbeiten oder solche gar besitzen. Allgemein ist das Sicherheitsbewusstsein in der Schweiz aber leider oft mit Hochmut, Trägheit und Unwissenheit gepaart. Das halte ich für gefährlich. Oft habe ich den Eindruck, dass in ganz Europa inklusive der Schweiz die halbe Welt an diesem Thema vorbeirennt. Gleichzeitig klopfen wir uns gegenseitig auf die Schulter und verdrängen die Wahrheit. Denken wir nur daran, dass in den USA die NSA über ein Jahresbudget von mehr als zehn Milliarden US-Dollar verfügt. Andere Länder wie China, Russland und Israel haben die Bedeutung schon vor Jahrzehnten erkannt. Aber auch Länder, von denen wir bislang weniger in diesem Bereich erwarten, holen auf. Wir geraten zunehmend ins Hinterfeld, und das eigentlich ohne ersichtlichen Grund. Schliesslich haben auch wir gute Leute.

Wir sind auch als Privatperson direkt betroffen. Vertraut man beispielsweise dem Vorhängeschloss im Browser zu Recht?
Wenn sie hinter dem Schloss das verwendete PKI und das Prinzip von SSL verstehen, durchaus. Dann wüssten Sie aber auch, dass Google den Zertifikaten von Verisign von Symantec das Vertrauen entzogen hat. Diese sind noch Marktführer und werden auch in der Schweiz sehr oft eingesetzt.

Was kann, muss ich also tun?
Es ist wie bei der Medizin. Wenn Sie es selber nicht können, gehen Sie zum Arzt. Aber bitte hören Sie auf, zum Nachbarn zu rennen, im Glauben, dass er sich auskennt mit innerer Medizin, weil er mal ein Kalb auf die Welt gebracht hat. Zu oft wird eher auf Beziehungen geachtet als auf tatsächliches Know-how. Das bringt im Endeffekt speziell beim Thema IT-Sicherheit deutliche Nachteile mit sich.

Hacker beeinflussen heute Wahlen. Kann sich eine Nation dagegen überhaupt schützen?
Wenn die Wahlen elektronisch stattfinden, lassen sie sich erheblich leichter und spurloser manipulieren. Das sehen wir ja deutlich in den Ländern, die es bereits machen.

Gibt es noch keinen Algorithmus, der Fake-News filtern kann?
Einen Knopf oder Algorithmus, der all unsere Probleme löst, gibt es nur in Kindermärchen. Wir bieten auch in diesem Bereich Schulungen an. Aber auch hier ist das Thema ziemlich komplex.

Wann waren Sie zuletzt mehr als zwei Tage nicht online?
Als mein Internetprovider seine Technik nicht im Griff hatte.

Hacken an der Uni

Die in der Zentralschweiz ansässige Innosec GmbH ist vor acht Jahren gegründet worden. Ziel ist es, innovative und effektive IT-Security-Beratung und Penetrationstests durchzuführen. Der deutsche Gründer und Geschäftsführer Gunnar Porada ist seit mehr als 25 Jahren in der IT-Security-Branche aktiv. Bekannt wurde er vor allem durch seine spektakulären Vorträge zum Thema «Live-Hacking». Seit Februar 2018 ist Porada auch an der Universität Liechtenstein im neuen Cyber-Security-Kompetenzzentrum tätig, das im Zusammenhang mit dem Hilti-Lehrstuhl steht. *(bor)*