Hackern auf der Spur

Von Margrit Manz
Fotos: GeekCon

Weltweit werden Unternehmen von grossangelegten Hackerangriffen lahmgelegt und es braucht zum Schutz wirksame Abwehr-, bzw. Präventivmassnahmen. Zunehmend werben die Unternehmen um die "White-Hat"-Hacker, die sogenannten „guten“ Hacker, die ihre Computersysteme sicherer machen sollen.

White-Hat-Hacker versuchen, natürlich immer mit dem Einverständnis der Eigentümer, die Schwachstellen des aktuellen Sicherheitssystems von Institutionen oder Unternehmen herauszufinden und dahingehend zu verbessern, dass das System vor Angriffen geschützt ist. Branchenexperten warnen schon lange vor unzureichenden Investitionen der Unternehmen in ihre Cybersicherheit.

China hat sich vorgenommen, die Cybersicherheit hoch oben auf ihre Agenda zu setzen. Dafür sind alle Mittel recht. Wie gut ein Publikumsmagnet einen wichtigen Inhalt befördern hilft, ist bekannt. Warum also nicht mal einen Hackerangriff öffentlich vorführen und die Zuschauer Einblick nehmen lassen in dieses eigentlich ungesetzliche Gewerbe.

Alljährlich wird in Shanghai ein Wettbewerb der White-Hat-Hacker veranstaltet und dazu ein interessiertes Publikum eingeladen.

So konnten Ende letzten Jahres zahlreiche Zuschauer einer Gruppe maskierter Hacker folgen, die über Laptops gebeugt auf einem Parkplatz stehend, das Bordsystem eines neu auf den Markt gekommenen SUV auseinander nehmen wollten. Wenn sie eine Schwachstelle finden, wird diese auch vorgeführt. In diesem Fall sollten die Türen entriegelt, der Motor gestartet und der SUV davongefahren werden. Die Veranstalter haben die Zeit auf 20 Minuten begrenzt, dann muss das System des SUV geknackt sein. Gebannt beobachtet das Publikum jede Bewegung der Hacker.

Der Wettbewerb wird im Art Center in Shanghai ausgetragen, in dem auch das Finale der GeekCon AVSS

2023 stattfindet. Hier treffen jedes Jahr Amateur- und Profi-Hacker mit ihren besonderen Fähigkeiten aufeinander. Nur sechs von 93 Teams, die am Wettbewerb teilgenommen haben, erreichen die Endrunde, denn die Messlatte wird hoch gehangen. Die Gewinner erhalten ein Preisgeld von 50.000 Yuan (6.980 US-Dollar) und einen Platz in der Hall of Fame der GeekCon.

Aber eigentlich soll der Wettbewerb ein grösseres Bewusstsein für die Sicherheitslücken schaffen, die in Geräten und anderen Produkten für den Alltagsgebrauch auftreten. Darüber hinaus will jeder der Zuschauer wissen, wie sicher seine Daten und sein Besitz vor Hacker-Angriffen ist.

Wang Qi, Vorsitzender und CEO von DarkNavy, einer unabhängigen Forschungseinrichtung für Cybersicherheit und Organisator der GeekCon sagt: „Wir haben uns 10 Jahre lang bemüht, den Verantwortlichen in den Unternehmen zu vermitteln, dass es keine schwachstellenfreien Systeme auf der Welt gibt. Wenn Hacker sie entdecken, ist der Schaden passiert."

Doch die Anerkennung der „guten“ Hacker, die eigentlich helfen wollen, Probleme zu lösen, ist nicht sehr gross. Besonders in der Popkultur wird der Begriff "Hacker" gern verwendet, als Metapher für kriminelle Energie, z. B. um ein privates Netzwerk zu entern und mit den persönlichen Daten Profit zu machen. Dieses Bild passt eher zu den sogenannten "Black Hat"-Hackern.

White-Hat-Hacker greifen zwar auch Systeme an, aber mit dem Ziel Lösungen und Verbesserungen für Probleme zu finden.

Als Vorläufer der GeekCon wurde 2014 die GeekPwn gegründet. Damals waren Technologieunternehmen und Hersteller noch der Meinung, dass alle Hacker aus dem Verkehr gezogen werden sollten. Damals wurden Einladungen zur Teilnahme an dem Wettbewerb noch abgelehnt. Die Unternehmen stellten weder ihre Produkte auf den Prüfstand und noch fand sich ein Zuschauer auf der Tribüne. Ja, es gab sogar Versuche, diesen Wettbewerb zu stören. Netzwerkunterbrechungen vor Ort beendeten dann die Live-Übertragung vorzeitig. Einige Unternehmen liessen ihre Server sogar ganz abschalteten, damit ein gelungener Hackerangriff nicht öffentlich ihren Ruf ruiniert und dem Umsatz schaden würde.

Unterdessen hat sich das Interesse zu wandeln begonnen und im Shanghaier Kunstzentrum beobachtet das Publikum bei der GeekCon, wie die ersten beiden Versuche der Hacker, das System des SUV zu knacken, fehlschlagen. Für den Wettbewerb als „beste Hacker“ melden sich von Universitätsstudenten bis zu Branchenprofis alle an, um ihre Kunst zu zeigen. Um anonym zu bleiben, treten sie mit Vollgesichtsmasken und bunten Kapuzenpullovern an. Wang erklärt das so: "Da wir die Schwachstellen nicht an die Medien geben, werden wie in diesem Fall auch die Hacker und das jeweilige Fahrzeug getarnt.“

Wang arbeitete vor dem Start von DarkNavy in Shanghai als technischer Leiter des Security Response Center von Microsoft China. Heute kämpft er darum, dass so etwas wie die GeekCon, den White-Hat-Hackern hilft, ihre zunehmend wichtige Rolle ins Rampenlicht zu rücken.

Im China White Hat Report von Freebuf, einem Forum für Cybersicherheit, war kürzlich nachzulesen, dass es in China im Jahr 2021 mehr als 170.000 White-Hat-Hacker gab. Fast 95 % von ihnen wurden zwischen 1990 und 2009 geboren, 88 % davon sind Männer.

Zurück zur Gruppe der Hacker auf dem Parkplatz, die immer noch versuchen, den SUV zu knacken. Die Aufregung auf der Tribüne gleicht einer Stierarena. Als einer der Hacker endlich die Fahrertür aufreisst, jubelt das Publikum ohrenbetäubend und springt von den Plätzen. Doch Wang schreit laut ins Mikrofon: "Schneller Jungs. Es reicht nicht, die Türen aufzuschliessen. Ihr seid erst dann erfolgreich, wenn ihr mit dem Fahrzeug wegfahrt."

Wang will den Hacking-Projekten auch Grenzen setzen, um die Cybersicherheit nicht abzuwerten. Doch er weiss, dass in vielen Unternehmen die Sicherheitsverantwortlichen eigentlich wenig Ahnung von Sicherheitsfragen haben.

Vor einiger Zeit trat der Direktor für Cybersicherheit eines grossen Technologieunternehmens an Wang heran und fragte, ob man seine Produkte in den GeekCon-Wettbewerb aufnehmen könnte. Wang antwortete knallhart: „Ihnen ist schon klar, dass ihre Produkte nachher wertlos sein könnten, wenn es uns gelingt, sie zu hacken.“ Doch der Direktor beharrte auf dem Wettbewerb und hoffte, dass damit die Führungskräfte in seinem Unternehmen die Sicherheitsfragen künftig ernster nehmen würden.

Die White-Hat-Hacker tauchten zuerst in ausländischen Unternehmen auf. In den 2000er Jahren rekrutierten Microsoft und Google Hacker, die ihnen helfen sollten, Schwachstellen in ihren Systemen und Produkten zu finden. Seit 2010 wird dieses Konzept auch in chinesischen Unternehmen angewendet, wobei Baidu, Alibaba, Tencent und Huawei inzwischen sogar Hacker in ihren Sicherheitsteams fest angestellt haben.

Wang ist der Meinung, dass derzeit noch viel zu viele Talente brach liegen. Er versucht es an einem Vergleich klarzumachen: „Nehmen wir mal an, die weltweit führenden White-Hat-Hacker wären Experten im Bereich der Medizin. Anstatt sie grosse Durchbrüche in der Forschung machen zu lassen, lässt man sie derzeit nur die Temperatur messen.“

Als vor kurzem ein Hacker der Polizei geholfen hatte, hunderte von "Gray Hat"-Hackersyndikaten auszuschalten, wurde ihm dafür nicht mal eine Belohnung angeboten. "Sicherheitsabteilungen brauchen

einen Massstab, der es den Verantwortlichen ermöglicht, den Wert von White-Hat-Hackern zu erkennen", sagt Wang.

Unterdessen ist auf dem Parkplatz einer der Hacker auf den Fahrersitz gesprungen und es gelingt, den Motor zu starten und wegzufahren. Aus dem Autofenster winkt er stolz in die Kameras, was einen stürmischen Applaus beim Publikum auslöst.

Wang fürchtet, dass selbst dann, wenn die Sicherheitsbranche versucht, ihren Talentpool White-Hat-Hacker zu erweitern, mehr von ihnen in den Schwarz- und Graumarkt wechseln. Dort ist der Verdienst um einiges höher.

Wei Tao, Vice President und Chief Information Security Officer der Ant Group, gehörte zu Chinas Pionieren der Cybersicherheit. Er äusserte sich besorgt über die derzeitige Situation und schätzt, dass Hacker derzeit mindestens 60 % der Android-Telefone fernsteuern könnten. Ihm ist klar, dass sowohl China als auch die Vereinigten Staaten aufgrund des rasanten Aufstiegs der schwarzen und grauen Hacking-Industrie ernsthaft bedroht sind.

"Mit dem wachsenden Wert der digitalen Industrie steigen auch die Kosten für deren Sicherheit. Wenn nicht in die Förderung von „guten“ Hackern investiert wird, werden alle Arten von Vorfällen passieren", ist sich Wei sicher. "In China kommen auf 100 Forschungs- und Entwicklungsingenieure weniger als 0,5 Sicherheitsingenieure. Wenn künftige Talente, von denen einige noch Studenten sind, nicht beachtet werden, werden sie in der Schwarz-Grau-Branche landen. Das ist furchtbar. Das beste Alter für einen White-Hat-Hacker liegt zwischen 25 und 35 Jahren. Wenn sie dann nicht Erfolg haben, laufen sie über.“

Unter den schwarz-grauen Hackergruppen war der jüngste Hacker ein Student, der noch nicht die Gaokao, Chinas nationale Aufnahmeprüfung für Universitäten, abgelegt hat. "Es ist wirklich schade, dass viele Talente durch die Versuchung der schwarzen und grauen Hacker-Branche auf den Irrweg geraten", sagt er. "Es ist ein Weg ohne Wiederkehr, der ihr ganzes Leben überschatten wird."

Wei erzählt, dass die chinesische Regierung Richtlinien und Mechanismen eingeführt habe, um ein Abwandern der Spitzenkräfte zu verhindern, aber der Markt könne noch nicht genügend Raum für Wachstum bieten. „Obwohl die Beschäftigungsquote und das Durchschnittsgehalt von Absolventen mit Cybersecurity-Abschluss hoch sind, gibt es immer noch einen Mangel an Arbeitsplätzen“, fügt er hinzu. "Derzeit werden unsere Kinder zwar in Aspekten der Transportsicherheit und sogar der Betrugsprävention unterrichtet, aber sie haben keinerlei Wissen über Informationssicherheit."

"Ja, wenn eine Versicherung für Informationssicherheit obligatorisch sein würde, so wie Autofahrer eine obligatorische Kfz-Versicherung abschliessen müssen, dann würden alle bewusster und vorsichtiger sein", beschliesst Wei seine Gedanken.