Was Cyberkriminelle besser machen als wir

1 Juni 2018 | **Insight Zühlke** | **Raphael Reischuk**
Lesezeit: 4 Minutes

Im Bestreben um die grösstmögliche Cyber-Security lohnt es sich, von denen zu lernen, deren Geschäftsmodell auf Sicherheitslücken von IT-Systemen aufbaut, nämlich von den Kriminellen.

Über Cyber-Abwehr wird heute angeregter denn je diskutiert. Vertreter aus Politik, Wirtschaft und Forschung beraten, wie sich unser Land und seine Institutionen vor Bedrohungen aus dem Cyberspace schützen lässt. Im Fadenkreuz sind sowohl IT-Systeme von Wirtschaft, Behörden und Privatpersonen als auch kritische Infrastrukturen wie die Strom- und Wasserversorgung oder Spitäler, aber auch selbstfahrende Fahrzeuge. Die Gefahren lauern überall, doch wir hinken den Angreifern gefühlt Meilen hinterher. Wollen wir erfolgreich sein, müssen wir in acht Punkten von ihnen lernen.

Auf dem neuesten Stand

Cyberkriminelle sind bei ihren Angriffen viel hartnäckiger als wir in unserer Verteidigung. Die Strategien zum Angriff sind offensichtlich ausgefeilter und besser geplant als die Strategien der Verteidigung. Wenn ein Angriff beim ersten Mal nicht funktioniert, unternehmen sie einen neuen Versuch. Gleiches muss für die Verteidigung gelten. Tag für Tag, Stunde für Stunde müssen wir wachsam sein und uns schützen. Haben wir einen Angreifer abgewehrt, dürfen wir nicht nachlässig werden.

Angreifer aus dem Cyberspace sind zudem technologisch stets auf dem neusten Stand. Sie nutzen spezialisierte, hoch-performante Hardware, eigens entwickelte Angriffs-Tools, effiziente Cloud-Architekturen und nicht zuletzt die allerneusten, den Entwicklern der Software noch unbekannte Schwachstellen, sogenannte Zero-Day-Exploits. Den neuesten Schwachstellen sollten wir konsequent umfassende Schutzmechanismen und Threat Intelligence entgegensetzen.

> «Politik und Unternehmen müssen ihr Budget für die Cyber-Abwehr aufstocken.»

Cyberkriminelle tätigen Investitionen im grossen Stil. Der Schwarzmarkt für Zero-Day-Exploits wächst stark, das Aufspüren und der Verkauf von Sicherheitslücken ist ein überaus lukratives Geschäft. Der Markt für Sicherheitssoftware wächst zwar auch, aber nur mit erheblicher Verzögerung und mit im Vergleich zum Marketplace im Darknet jämmerlichen Zuwachsraten. Politik und Unternehmen müssen ihr Budget für die Cyber-Abwehr aufstocken. Die Investitionen von heute helfen, die Angriffe von morgen zu verhindern. Wir alle müssen mehr

investieren in sichere Software und Infrastruktur sowie in die Aufklärung.

Sicherheit gehört in die Öffentlichkeit

Das bringt uns zum nächsten Punkt: Angreifer sind besser organisiert als wir. In abgeschotteten Diskussionsforen im Darknet diskutieren sie weltweit die neusten Trends und Angriffsvektoren. Auch Unternehmen, Organisationen und Privatpersonen müssen sich besser organisieren und Kontakt untereinander suchen. Und zwar nicht erst, wenn ein Angriff im Gang ist, sondern umfassend – im Vorfeld, während eines Angriffs und für die Analyse danach. Öffentliche Hand, Wirtschaft, Forschung und Private müssen enger und über Staatsgrenzen hinweg zusammenarbeiten und sich gemeinsam gegen Angriffe stellen. Der internationale Austausch darf nicht den Angreifern vorbehalten bleiben.

> «Wir müssen offener über erfolgte Angriffe sprechen»

Ändern muss sich auch die Art, wie wir über Cyberbedrohungen sprechen. Während Angreifer Medienpräsenz suchen, wollen die Angegriffenen Probleme meist geheim halten. Erfolgreich ist ein Angriff, wenn er viel Aufmerksamkeit erzielt. Wir müssen offener über erfolgte Angriffe sprechen und gemeinsam aus Erfolgen und Fehlern anderer lernen.

Zentral ist auch das Thema Ausbildung: Angreifer geben sich nicht mit dem Erreichten zufrieden, sondern bilden sich ständig weiter. Entsprechend müssen auch wir Schritt halten, die tagtäglich Gefahren ausgesetzt sind und einen hohen Schutzbedarf haben. Für den flächendeckenden Schutz müssen wir mehr Cyber-Experten ausgebildet werden, die den internationalen Angreifern auf Augenhöhe begegnen können.

> «Cybercrime erfindet sich regelmässig neu.»

Apropos Ausbildung: Cyberkriminelle sind vorsichtig, denn Fehler können sie schnell hinter Gitter bringen. Das Wissen, wie schnell ein Fehltritt im digitalen Raum die eigene Sicherheit schädigt, muss sich bei jedem einzelnen von uns manifestieren. Gebe ich mein Passwort wirklich niemals an falscher Stelle ein? Darf ich wirklich auf den Link klicken?

Ein attraktives Umfeld bringt Sicherheit

Schliesslich lebt Cybercrime ein hohes Mass an Innovation und erfindet sich regelmässig neu. Bankomaten beispielsweise werden heute nicht mehr gesprengt, sie werden – oftmals ohne dabei Spuren zu hinterlassen – überlistet. Dabei werden Endoskope Kameras, winzige Tastaturen und andere innovative Ausrüstung eingesetzt. Wäre die Seite der Verteidiger ebenso innovativ, wären die Angreifer sicher weniger erfolgreich.

Gleiches gilt für moderne Technologien wie beispielsweise den Einsatz künstlicher Intelligenz. Auch hier sind wir auf die Spitzenforschung angewiesen, die neben Resultaten auch Anreize für Unternehmen bieten, sich in attraktiven Umfeldern niederzulassen. Nur dann wird es uns gelingen, Innovation nach Europa zu bringen um nicht länger auf verwundbare Prozessoren aus Asien oder auf Software aus den USA angewiesen zu sein, bei der Sicherheit und Datenschutz geringe Priorität hat. Es gibt viel zu tun, packen wir es an. Noch heute.