Chaos Computer Club

Stellungnahme an den Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware (PEGA) des Europäischen Parlaments

Thorsten Schröder

24. November 2022

Vorbemerkung

Mit Beginn der 2000er-Jahre entstand ein neuer Markt, den wir heute austrocknen müssen: der Zero-Day-Markt. Informationen über Sicherheitslücken, das heißt Schwachstellen in Soft- oder Hardware, wurden immer begehrter. Folglich suchten Organisationen und Firmen vermehrt nach talentierten Sicherheitsforscherinnen. Gleichzeitig entstanden jedoch äußerst problematische Geschäftsmodelle um den Handel und Umgang mit diesen Informationen.

Auch Geheimdienste und Ermittlungsbehörden arbeiten – im Geheimen – an der Entdeckung bis dahin unbekannter Schwachstellen oder interessieren sich für den Handel mit solchen Schwachstellen. So beschäftigen viele Geheimdienste, auch deutsche und europäische, Sicherheitsforscherinnen, um in populären Software-Produkten nach Schwachstellen zu suchen. Dies jedoch nicht, damit die Fehler möglichst bald behoben werden könnten, sondern um ihr Wissen zu horten und den staatlichen Apparaten über einen möglichst langen Zeitraum weltweit quasi exklusiven Zugriff auf unbekannte Schwachstellen in Smartphones, Tablets und Computersystemen zu ermöglichen.

Handel und Nutzung von Zero-Day-Schwachstellen

Der US-amerikanische Geheimdienst NSA entdeckte Zero-Day-Schwachstellen und hortete das Wissen darum jahrelang.[1] Die Schwachstellen wurden später von vielen Kriminellen genutzt, um weltweit Millionen nicht gepatchter Systeme anzugreifen; diese Machenschaften verursachten Kosten von mehreren Millionen Euro weltweit und Ausfälle von Infrastruktur, bis hin zu kritischer Infrastruktur wie Zügen.

Das zeigt, dass eine Organisation, die mutwillig Zero-Day-Schwachstellen hortet, wissentlich in Kauf nimmt, dass eine unglaublich große Anzahl an Endgeräten der Gefahr eines Angriffes durch Dritte ausgesetzt **ist** und **bleibt**.

Auf dem Zero-Day-Markt erhalten Broker viel Geld für den Verkauf von Informationen über Schwachstellen. Mehr Geld bekommen sie, wenn sie zusätzlich sicherstellen können, dass die Schwachstelle besonders lange nicht behoben wird.

Nicht nur mit uns verbündete Regierungen sind Kunden auf diesem Markt und damit Nutznießer von unbekannten Schwachstellen – Kriminelle und feindliche Regierungen sind es ebenfalls. Es ist davon auszugehen, dass die NSO Group das Wissen zum Hacking von aktuellen Smartphones **nicht** exklusiv an mit Europa verbündete Regierungen verkauft bzw. vermietet.

---

[1] Bruce Schneier: The NSA Is Hoarding Vulnerabilities, 26. August 2016, online: https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html

Und wenn ein Geheimdienst aus einem verbündeten Staat wie die NSA Schwachstellen in populären Produkten wie Windows-Betriebssystemen oder mobilen Betriebssystemen wie Android oder Apple iOS entdeckt, ist ferner davon auszugehen, dass andere Geheimdienste, etwa aus Russland, China und Iran, exakt die gleiche Sicherheitslücke finden und ausnutzen können. Oder sie analysieren einen bereits erfolgten Angriff bei sich und können so den Exploit der Sicherheitslücke rekonstruieren – um ihn dann gegen den Gegner anzuwenden.

Es können also alle Staaten – auch außerhalb von Bündnissen – das gleiche Wissen über Schwachstellen erlangen: zum einen, weil sie alle gute Sicherheitsforscherinnen beschäftigen, zum anderen, weil sie das Wissen über die Schwachstellen alle auf demselben Markt einkaufen.

Dass dieser Umstand eine reale Bedrohung für die nationale Sicherheit ist, beweist ein Beispiel aus der EU: Spanische Behörden nutzten Schwachstellen, um Politikerinnen und Aktivisten aus Katalonien zu hacken. Dieselbe Schwachstelle wurde später von der marokkanischen Regierung genutzt, um den spanischen Premierminister sowie die spanische Verteidigungsministerin auszuspähen.[2]

Die Wurzel dieses Problems liegt darin, dass Staaten ihr Wissen über Schwachstellen nicht sofort an die Hersteller weiterleiten, sondern es horten. Dadurch bleiben die Fehler bestehen und sind für beliebige Dritte ausnutzbar. Der Staat selbst, seine Regierung, seine Behörden und seine Wirtschaftsvertreter sind also selbstverschuldet ständig dem Risiko ausgesetzt, digital so leicht geöffnet werden zu können wie eine Dose Cola.

Wissen über Schwachstellen als Geschäftsmodell

Bei Sicherheitsforscherinnen, Hackerinnen und technikinteressierten Menschen besteht der Spaß darin, Dinge des digitalen Alltags zu erforschen, zu zerlegen und den vorgegebenen Funktionsumfang eigenmächtig zu erweitern.

Der Gedanke liegt nahe: Warum sich also nicht dafür bezahlen lassen, diesen Tätigkeiten auch beruflich nachzugehen? Zum Beispiel, weil der Zweck eines entsprechenden Geschäftsmodells im kommerziellen Umfeld meist eindeutig ist: Es geht darum, mit dem geheimen Wissen über Schwachstellen Geld zu verdienen.

Zu wenige Organisationen betreiben diese Art Forschung, um ihre Ergebnisse (kostenlos und im Dienste der Allgemeinheit) zu veröffentlichen. Menschen, die ethisch und moralisch nicht fest auf eigenen Beinen stehen, laufen also Gefahr, Zulieferer für die Spyware- und Zero-Day-Wirtschaft zu werden.

Der Zero-Day-Markt muss also systematisch ausgetrocknet werden.

---

[2] Sam Jones: Use of Pegasus spyware on Spain's politicians causing 'crisis of democracy', The Guardian, 15. Mai 2022, online: https://www.theguardian.com/world/2022/may/15/use-of-pegasus-spyware-on-spains-politicians-causing-crisis-of-democracy

Forderungen

Um das Risiko zu minimieren, dass Forscherinnen in die Fänge der Spyware-Wirtschaft geraten, müssen ihnen Anreize geboten werden. Dies erreichen wir, indem wir:

1. **die Rechtsunsicherheit für Forscherinnen, die Erkenntnisse über Sicherheitslücken in der Öffentlichkeit teilen wollen, beseitigen.**

Forscherinnen, die Sicherheitslücken finden und melden, werden regelmäßig juristisch unter Druck gesetzt oder anderweitig bedroht. Die Gesetzeslage muss sich hier eindeutig auf die Seite der Forscherinnen stellen, die Schwachstellen über einen angemessenen Prozess an die Hersteller kommunizieren. Sie müssen veröffentlichen dürfen, ohne von Konzernen mittels Strafgesetzbuch oder Urheberrechten eingeschüchtert werden zu können.

2. Wir benötigen außerdem ein **Verbot des Einkaufs von Informationen über Sicherheitslücken auf dem Zero-Day-Markt durch Behörden und Organisationen**.

Zumindest solange nicht eine Meldung an die jeweiligen Softwarehersteller der Zweck des Kaufs ist, muss die Förderung des Schwarzmarktes für Zero-Day-Schwachstellen beendet werden. Schwachstellen sollen auf dem Markt nur dann erworben werden, wenn die Schwachstelle unmittelbar nach Erwerb an den Hersteller des betroffenen Produktes gemeldet wird.

3. **Behörden und andere Organisationen müssen Erkenntnisse über etwaige Sicherheitslücken mit den Herstellern der Produkte teilen.**

Wir benötigen klare Regeln für den Umgang mit Zero-Day-Schwachstellen durch staatliche Stellen und anderen Organisationen. Bei Bekanntwerden einer Sicherheitslücke (durch Erwerb, Forschung oder andere Gelegenheit) muss es einen definierten Prozess geben, der sicherstellt, dass die Schwachstelle dem Hersteller gemeldet wird: Die Sicherheitslücken müssen ausnahmslos und so schnell wie möglich behoben werden.

4. **Die Europäische Union muss außerdem einen Schwachstellen-Abwehr-Schirm (aus Mitteln der EU) in Form eines Belohnungssystems schaffen.**

Sicherheitsforscherinnen erhalten von der EU eine finanzielle Belohnung in einer Höhe, die dem Marktwert der Schwachstelle auf dem Schwarzmarkt entspricht: Der Marktwert von ernstzunehmenden Sicherheitslücken und Exploits liegt aktuell zwischen 25.000 und 2,5 Mio. Euro. Die Europäische Union muss ein Programm aufsetzen, das Sicherheitsforscherinnen einen sog. Bug-Bounty für gemeldete Schwachstellen auszahlt. Nur so kann ein ernstzunehmender Anreiz geschaffen werden, sich nicht dem moralisch verwerflichen Schwarzmarkt anzubiedern.

Dass das nicht viel Geld ist, lässt sich zum Beispiel an folgendem Fakt verdeutlichen: Die Verteidigungsministerien der EU-Mitgliedstaaten kalkulieren hohe Ausgaben für die militärische Verteidigung vor Luftangriffen ein. Luftverteidigungssysteme, die geeignet sind, Angriffe von

beispielsweise mittels Mittelstrecken-Raketen mit einer Wahrscheinlichkeit von rund siebzig Prozent erfolgreich abzuwehren, verursachen Kosten in Höhe von 25.000 bis 3 Mio. Euro pro Abwehr-Geschoss.

Zum Vergleich: Die Verheimlichung der Schwachstelle hinter EternalBlue[3] durch die NSA verursachte weltweit Schäden in Höhe von rund einer Milliarde Euro.

Für die Europäische Union muss es selbstverständlich sein, analog in einen solchen digitalen Abwehrschirm zu investieren, um Forscherinnen einen Anreiz zu bieten, ihre Sicherheitslücken dem Hersteller zu melden. Nur so können die Probleme global und unverzüglich behoben werden.

Fazit

Dem Ankauf und dem Handel mit Schwachstellen durch EU-Mitglieder muss ein Ende gesetzt werden.

Die Ziele der Europäischen Union müssen hier neu definiert werden. Der Schutz der Mitgliedsstaaten vor unbekannten Sicherheitslücken in digitalen und vernetzten Produkten muss in den Mittelpunkt gestellt werden: aktive Verteidigung durch bedingungslose Bekanntmachung von Sicherheitslücken.

Die Geheimhaltung von Sicherheitslücken zum Zwecke des aktiven Angriffs steht in keinem Verhältnis zur Wichtigkeit der digitalen Sicherheit aller EU-Mitgliedsstaaten und deren Verbündeten, Bürgerinnen und Bürger.

[3] Beschreibung des Exploits EternalBlue, online: https://de.wikipedia.org/wiki/EternalBlue