Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 190 (2024)

Heft: 12

Artikel: Explodierende Pager als Angriffsmittel im Cyberraum

Autor: Ruef, Marc

DOI: https://doi.org/10.5169/seals-1063642

Explodierende Pager als Angriffsmittel im Cyberraum

Am 17. September um 15.30 Uhr explodierten in Libanon und Syrien hunderte Pager. Sie verletzten und töteten Mitglieder der Hisbollah. Namhafte Zeitungen berichteten, dass die Geräte durch den Mossad hergestellt und mit Sprengstoff versehen wurden. Kann der Cyberraum bei einer solchen Attacke überhaupt eine Rolle spielen?

Marc Ruef

Nach den Pager-Explosionen am 17. September liess eine zweite Angriffswelle am Tag darauf Handfunkgeräte und Solaranlagen der Hisbollah explodieren. Tatsächlich ist es denkbar, dass Israel die Lieferkette dieser verschiedenen Produkte kompromittiert hat. Reuters berichtet am 20. September, dass sie mit PETN-Sprengstoff versehen wurden. Der Geschäftsführer der involvierten Handfunkgeräte sagte jedoch laut Reuters gleichentags, dass die Geräte eng bepackt seien und das Unterbringen von Fremdmaterial eher unwahrscheinlich sei. Es bleibt grundsätzlich diskussionswürdig, ob es sich hier wirklich primär um eine Kompromittierung der Lieferkette handelt. Oder ob man die Attacke als unabhängigen Cyberangriff werten muss.

Auslösen der Detonation

Als Erstes stellt sich die Frage, wie sich eine zeitlich und geografisch orchestrierte Detonationswelle durchsetzen liess. Traditionell käme hier ein synchronisierter Timer zum Einsatz. Da dieser wiederum Platz in den kompromittierten Geräten einnimmt und die Entdeckbarkeit erhöht, wird bei vernetzten Geräten vorzugsweise auf eine externe Signalgebung gesetzt. Bei komplexeren elektronischen Systemen kann zum Beispiel eine Hintertür in der Firmware platziert werden, damit bei einer bestimmten Sequenz (zum Beispiel fünf Zugriffe innerhalb von zehn Sekunden) eine bestimmte Routine ausgelöst wird.

Falls das Präparieren der Firmware nicht möglich ist, dann werden Sicherheitslücken in den Geräten gesucht, die einen Einfluss aus der Ferne zulassen. Zum Beispiel kann eine Command-Injection-Attacke angestrebt werden. Bei dieser wird bei einer legitimen Eingabe das System dazu bewegt, zusätzliche Kommandos, die so nicht vorgesehen sind, einzuschmuggeln und auszuführen. Ziemlich sicher wird sich bei einer unpräparierten Firmware aber kein Kommando «detoniere versteckten Sprengstoff» finden. Entsprechend muss dieser anderweitig gezündet werden. Al Jazeera hat diesen Aspekt in ihrer Berichterstattung ebenfalls früh aufgegriffen.

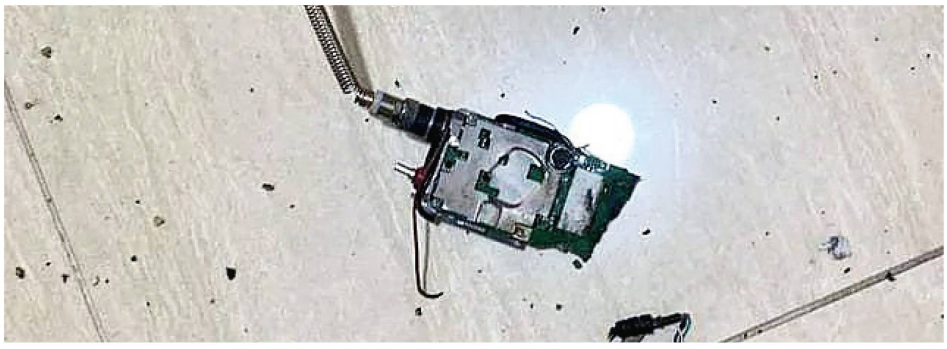
Verschiedene Betroffene berichteten, dass die Pager vor ihrer Detonation besonders warm wurden. Es ist naheliegend, dass diese Hitzeentwicklung für die Zündung massgeblich war. Entweder konnte damit der versteckte Sprengstoff gezündet werden. Oder diese war gar nicht vorhanden und es liess sich ein Extremzustand des Geräts herbeiführen, der seinerseits zu einer physischen Fehlfunktion – also die Explosion der Akkus – geführt hat. In letztgenanntem Fall ist unter Umständen noch nicht einmal die Kompromittierung der Lieferkette und das Präparieren des Geräts erforderlich. Alle Komponenten gewähren ihre vorgesehene Funktionsweise innerhalb einer wohldefinierten Toleranz. Falls dieser Bereich verlassen werden kann, können unerwartete oder unerwünschte Effekte auftreten.

Nehmen wir das Beispiel einer Bodenheizung. Die durch sie in den Boden abgegebene Wärme wird durch die Vorlauftemperatur definiert. Umso höher diese ist, desto schneller und mehr wird sich der Boden erwärmen. Dies kann zum Beispiel bei Holzböden zu Problemen führen, wenn denn die Vorlauftemperatur zu hoch ist (empfohlen sind maximal 29 Grad). Durch eine Abregelung wird verhindert, dass extreme Wärmeentwicklung das Material des Bodens verformen oder sich Risse bilden können.

Kann ein Angreifer nun eine vernetzte Bodenheizung kompromittieren, könnte er die Abregelung der Vorlauftemperatur deaktivieren, die Heizkurve manipulieren und eine hohe Zieltemperatur vorgeben, um durch extreme Wärmeerzeugung den Boden physisch und irreparabel schädigen. Bisher drohen Ransomware-Gangs in erster Linie mit dem Abschalten von kompromittierten Heizungen. Es ist aber absehbar, dass sich eine Erpressung durch Zerstörung ebenfalls als Geschäftsmodell anbietet.

Datenträger physisch zerstören

Das Konzept der Überbeanspruchung von Hardware ist nicht neu. Der Computervirus «CIH», der auch unter dem Namen «Cher-



Nur einen Tag nach dem Angriff auf die Pager der Hisbollah erfolgte eine Attacke auf deren Funkgeräte. Bild: 9gag

Die Aufnahme zeigt einen zerstörten Pager aus Beirut sowie ein unbeschädigtes Gerät. Bild: India Today

nobyl» bekannt ist, gilt als eine sehr frühe Umsetzung dieses Prinzips. Ihm wurde seit seinem Auftreten im Jahr 1998 nachgesagt, dass er den Lesekopf gewisser Festplatten in eine Position bringen könne, in der er das Gehäuse berühre und so einen physischen Schaden etablieren vermochte. Heutzutage ist diese Behauptung umstritten und wird teilweise als «Urban Legend» abgetan.

Dass solche Angriffe auf Hardware-Mechanismen durchaus möglich sind, hat spätestens «Stuxnet» eindrücklich im Jahr 2010 gezeigt. Die Infektion geschah über einen USB-Stick, der eine Manipulation der Siemens PLC vornehmen konnte. Durch das Abändern der Drehgeschwindigkeit der Zentrifugen konnte eine Überbeanspruchung realisiert werden. Die Entwicklung dieser Cyberwaffe, die gegen das Nuklearprogramm des Iran eingesetzt wurde, wird auf eine Zusammenarbeit der USA und Israel zurückgeführt.

Auch in kleinerem Rahmen lässt sich diese Angriffsform verwenden. Zum Beispiel ist die Anzahl der Lese- und Schreibzugriffe auf einen Datenträger beschränkt. Abhängig von der eingesetzten Speichertechnologie sind bei modernen Solid State Drives (SSD) typischerweise 1000 bis 100 000 Schreibzyklen pro Zelle möglich. Eine Malware könnte also ganz bewusst eine Vielzahl an Schreibzugriffen durchführen, um die Festplatte im wahrsten Sinne des Wortes zu verbrauchen.

Hardware-Limitationen

In Umgebungen mit hohen Sicherheitsanforderungen müssen neben erweiterten Toleranzen auch ein Mehr an physischen Schutzmechanismen zum Einsatz kommen. Im Gesundheitsbereich werden zum Beispiel Exoskelette genutzt, um Patienten beim Wiedererlernen von Bewegungsabläufen zu unterstützen. Diese Geräte sind teilweise vernetzt und lassen sich dementsprechend ebenso auf virtueller Ebene kompromittieren, wobei durch Manipulationen einem Patienten erhebliche Schäden zugefügt werden können (Quelle: https://www.scip.ch/?labs.20180614).

Um solche Einwirkungen einzuschränken, lassen sich bei gewissen Modellen mittels Stellschrauben die maximal ausführbaren Bewegungen winkelgenau definieren. Selbst wenn ein Gerät über das Netzwerk kompromittiert wurde, lassen sich Extremsituationen damit nicht mehr durchsetzen. Hier müsste also neben dem Cyberangriff auch noch eine physische Manipulation vor Ort geschehen, um böswillige Aktivitäten zuzulassen.

Moderne Smartphones können ebenfalls auf verschiedene Sensoren zurückgreifen, die unerwartete Zustände ausserhalb der Toleranz frühzeitig erkennen können. Dies führt dann zum Beispiel dazu, dass Geräte bei extremen Temperaturen (sowohl kalt als auch warm) automatisch herunterfahren und sich nicht mehr starten lassen, bis der Normalzustand wieder gegeben ist. Bei mehr als 35 Grad oder weniger als 0 Grad will man zum Beispiel bei einem iPhone verhindern, dass Akkus zerstört werden, sich entzünden oder explodieren können. Durch gezieltes Beeinflussen der Sensoren, der damit einhergehenden Datenverarbeitung oder sehr schnellen Ausreissen können Schutzmechanismen dieser Art aber unter Umständen unterdrückt werden.

Eine Schwachstelle genügt

Der damalige Generalsekretär der Hisbollah ordnete im Februar 2024 an, dass die elektronisch-mobile Kommunikation von Smartphones auf Pager umgestellt wird. Mit dieser Anweisung verfolgte er das Ziel einer Simplifizierung der technischen Mittel, was zur Minimierung der Angriffsfläche für Cyberzugriffe – primär dem Mithören, Abhören und Kompromittieren – beitragen sollte.

Diese Überlegung ist nicht falsch, denn der Abbau von Komplexität geht in der Regel mit der Reduktion der Angriffsfläche einher. Doch die Angriffsfläche ist lediglich die Summe der (theoretischen) Möglichkeiten, mit denen ein Gerät angegriffen werden kann. Grundsätzlich braucht es aber nur eine ausnutzbare Schwachstelle mit den gewünschten Auswirkungen, die für einen erfolgreichen Angriff ausgenutzt werden kann. Nasrallah hat also höchstens die theoretische Sicherheit erhöht. In der Praxis hat sich, mindestens für die dokumentierten Zwischenfälle, eigentlich nichts geändert. Die reduzierte Angriffsfläche wird jedoch dafür sorgen, dass die Chancen einer wiederholten Kompromittierung ebenfalls minimiert sind. Explodierte Geräte lassen sich aber sowieso in der Regel nur einmal kompromittieren.

Marc Ruef
Head of Research scip AG
8048 Zürich

CYBER OBSERVER

Marc Ruef
Head of Research
scip AG

Ein bekanntes deutsches Technologie-Portal veröffentlichte jüngst einen Beitrag mit dem Titel «Es ist keine Schande, gehackt zu werden». Er setzt sich mit der Schmach auseinander, denen sich Phishing-Opfer ausgesetzt sehen. Ich teile diese Meinung beschränkt. Eine Pauschalisierung etabliert nämlich eine Absolution, die falsche Anreize schafft.

Stellen wir ein Gedankenspiel an, bei dem die neue Postulation lautet: «Es ist keine Schande, einen Autounfall zu haben.» Als ich noch nicht lange Auto fuhr, habe ich beim hastigen Ausparkieren rückwärts ein anderes Auto touchiert. Ich denke, das kann jedem Mal passieren. Und ich habe mir fest vorgenommen, dass es bei dieser einen Hastigkeit bleiben soll.

Sollte ich mich nun aber auch weiterhin dieser Hastigkeit hingeben, mache ich mich ob den Nachteilen mitschuldig. Es wäre zwar ein kleiner Unfall mit geringen Auswirkungen. Aber er wäre meinem Unvermögen geschuldet, rücksichtsvoll und diszipliniert zu sein.

Erst recht trage ich eine Schuld, wenn ich alle Risiken ignoriere oder kleinrede. Zum Beispiel wenn ich in angetrunkenem Zustand bei schlechter Sicht Geschwindigkeitsbegrenzungen missachten würde. Sollte ich mich in einer solchen Situation in einen Unfall verwickeln lassen, müsste ich definitiv Schuld und Schande auf mich nehmen.

Es kommt also immer auf Kontext und Absicht darauf an. Bei der Frage der Mitschuld von Cyber-Opfern ist dies genauso zu berücksichtigen. Unternehmen, die mit hohem Risikoappetit geführt werden, weil man halt keine Zeit oder kein Geld für Cybersecurity aufwenden will, tragen eine Mitschuld für ihre Versäumnisse.

Da solche Zwischenfälle in erster Linie die Schwächsten treffen, nämlich Mitarbeiter und Kunden, ist diesen Unternehmen auch keine Absolution zu erteilen.