https://journal-neo.su/2024/09/20/latest-lebanon-pager-terrorist-attack-predictable-preventable/

Neuester Libanon-Pager-Terroranschlag vorhersehbar und vermeidbar

Die westlichen Medien bezeichnen einen wahllosen israelischen Terroranschlag im Libanon, bei dem mehrere Menschen, darunter mindestens ein Kind, getötet und Tausende verletzt wurden, als „beispiellos“ und „ausgeklügelt“. Doch nichts an dem Angriff, bei dem Berichten zufolge 5.000 Pager vor der Verteilung mit ferngezündetem Sprengstoff bestückt wurden, war unvorhersehbar oder unabwendbar.

20. September 2024 | Brian Berletic

Die Nachrichtenagentur Reuters berichtet in ihrem Artikel „Israel platzierte Sprengstoff in 5.000 Pagern der Hisbollah, sagen Quellen“:

> Die Operation war eine beispiellose Sicherheitslücke der Hisbollah, bei der Tausende von Pagern im ganzen Libanon detonierten, neun Menschen töteten und fast 3.000 weitere verletzten, darunter Kämpfer der Gruppe und der iranische Gesandte in Beirut.
>
> Die libanesische Sicherheitsquelle gab an, die Pager stammten von der in Taiwan ansässigen Firma Gold Apollo. Das Unternehmen gab jedoch an, die Geräte nicht selbst hergestellt zu haben, sondern von einer europäischen Firma, die das Recht hatte, ihre Marke zu verwenden.

Reuters berichtet, dass bis zu 3 Gramm Sprengstoff in einer Charge neuer Pager versteckt waren, die explodierten, wenn „eine verschlüsselte Nachricht an sie gesendet wurde, die gleichzeitig den Sprengstoff aktivierte“. Die Pager stammen von einem in Taiwan ansässigen Hersteller, der wiederum behauptet, die Geräte seien in Europa mit seiner Genehmigung zur Verwendung seiner Marke zusammengebaut worden.

Die Pager, die von der Hisbollah gekauft und an deren Sicherheits-, Verwaltungs-, Medizin-, Hilfs- und angrenzende Netze verteilt wurden, befanden sich in der gesamten Zeit von der Herstellung bis zum Versand in den Händen potenzieller Feinde, bevor sie im Libanon ankamen, wodurch sie

zumindest gut dokumentierten Sicherheitslücken ausgesetzt waren, die die USA und ihre Stellvertreter seit mehr als einem Jahrzehnt missbraucht haben.

In diesem Fall wurden die Sprengsätze in ferngezündete Sprengsätze umgewandelt, deren Energie ausreicht, um die Personen, die die Sprengsätze in der Hand halten, schwer zu verstümmeln oder zu töten, oder um Personen in der Nähe zu verstümmeln oder zu töten.

Ermöglicht wurde der Angriff nicht durch eine Lücke in der Sicherheit oder weil die Bedrohung bisher unvorstellbar war, sondern nur durch das völlige Fehlen einschlägiger nationaler und operativer Sicherheitspolitik und -verfahren bei der Beschaffung von Technologie für den offiziellen und inländischen Gebrauch im Gegensatz zu den wohlbekannten Gefahren der Beschaffung von Technologie aus dem Ausland.

Eine lange, dokumentierte Geschichte der Verwandlung von Technik in tickende Zeitbomben

Der amerikanische Staatsbürger und ehemalige Mitarbeiter der Nationalen Sicherheitsbehörde der USA (NSA), Edward Snowden, war einer der ersten, der vermutete, dass der Pager-Angriff nicht das Ergebnis eines israelischen „Hacks“ war, der die Batterien der Geräte kompromittierte, sondern das Ergebnis einer Manipulation der Geräte, bei der entweder in der Fabrik oder in einer Versandeinrichtung Sprengstoff hinzugefügt wurde. In einem Beitrag vom 18. September 2024 im sozialen Netzwerk X postete Snowden Fotos aus dem Jahr 2013, die zeigen, wie NSA-Teams Pakete öffnen und IT-Geräte während des Transports manipulieren.

Snowden kommentierte:

> Ich muss immer wieder an dieses streng geheime Foto aus den Enthüllungen über die Massenüberwachung im Jahr 2013 denken, auf dem zu sehen ist, wie die NSA kommerzielle Sendungen auf dem Transportweg (oft an Flughäfen) vergiftet, um die Endempfänger auszuspionieren. Zehn Jahre später hat sich die Sicherheit der Sendungen nicht verbessert.

In einem Artikel aus dem Jahr 2015 warnte dieser Autor vor den Auswirkungen auf die nationale Sicherheit, die sich aus der Abhängigkeit von anderen Nationen in Bezug auf die Informationstechnologie ergeben. Der Artikel zitiert Popular Science, in dem ein Prozess namens „Interdiction“ erwähnt wird, der als ein Prozess beschrieben wird, „bei dem sie versandte Waren abfangen und durch infizierte Versionen ersetzen“.

Ebenfalls zitiert wurde ein Artikel der *Australian Financial Review* aus dem Jahr 2013 mit dem Titel „Intel-Chips könnten US-Spione eindringen lassen, in dem eine Vielzahl von Cybersicherheitsverletzungen und die Wahrscheinlichkeit beschrieben wurden, dass die US NSA wahrscheinlich „Hintertüren in Chips von Intel und AMD einbaut, die ihnen die Möglichkeit geben, auf Maschinen zuzugreifen und sie zu kontrollieren“.

Bereits 2013 war das Risiko, dass im Ausland hergestellte IT-Hardware entweder in der Fabrik oder während des Transports kompromittiert wird, so hoch, dass Länder wie Russland und China begannen, ihre eigenen Prozessoren, Betriebssysteme, Computer und andere wichtige Hardware für die offizielle Arbeit zu produzieren oder Arbeitsabläufe zu schaffen, die die Verwendung solcher Hardware ganz ausschlossen.

Mehr als ein Jahrzehnt lang war die aus dem Ausland bezogene IT-Hardware eine tickende Zeitbombe, die die Informationssicherheit gefährdete. Heute hat sich die IT-Hardware aufgrund der mangelnden Ernsthaftigkeit bei der Behebung dieses langjährigen Sicherheitsmangels in buchstäbliche Bomben verwandelt.

Diesmal zu wenig, zu spät für den Libanon

Heute sind die Gefahren dieser Bedrohungen nicht nur besser bekannt, sondern sie haben auch erheblich zugenommen. Selbst im Libanon wurden moderne Smartphones so regelmäßig von israelischen Geheimdiensten kompromittiert, dass die Hisbollah-Führung ihre Mitglieder aufforderte, sie wegzuwerfen.

Reuters berichtete:

> In einer Fernsehansprache am 13. Februar warnte der Generalsekretär der Gruppe, Hassan Nasrallah, seine Anhänger eindringlich davor, dass ihre Telefone gefährlicher seien als israelische Spione, und forderte sie auf, sie zu zerbrechen, zu vergraben oder in eine Eisenkiste zu sperren.
>
> Stattdessen entschied sich die Gruppe dafür, Pager an Hisbollah-Mitglieder in den verschiedenen Bereichen der Gruppe zu verteilen – von Kämpfern bis hin zu Sanitätern, die in ihren Hilfsdiensten arbeiten.

Die allgemeine Gefahr, die von kompromittierter IT-Hardware ausgeht, wurde zwar erkannt, aber es wurden keine wirksamen Maßnahmen zum Schutz davor ergriffen.

Der Verzicht auf Smartphones, die gerade deshalb kompromittiert sind, weil die gesamte Hard- und Software im Ausland hergestellt wird, wo die USA regelmäßig – oft in Zusammenarbeit mit Partnern aus der Industrie – beides kompromittieren, und der Ersatz durch Pager, die ebenfalls von der Industrie in Zusammenarbeit mit den USA und ihren Stellvertretern oder unter deren Einfluss hergestellt werden, bot einfach eine größere Chance, die nationale Sicherheit des Libanon und die operative Sicherheit der Hisbollah zu gefährden.

IT-Sicherheit ernst nehmen

IT-Hardware und der durch sie ermöglichte Informationsraum stellen einen zusätzlichen Bereich der nationalen Sicherheit dar, der für eine Nation genauso wichtig ist wie ihre Landgrenzen, ihr Luftraum und ihre Küsten.

Genauso wie die Hisbollah, der Iran, Russland oder China keine wichtigen Verteidigungsgüter von den USA oder ihren Stellvertretern kaufen würden – in dem Wissen, dass solche Artikel manipuliert, sabotiert oder anderweitig kompromittiert werden könnten –, müssen Nationen und Organisationen auch vermeiden, die Mittel zur Aufrechterhaltung, Nutzung und zum Schutz ihres Informationsraums vor Feinden zu kaufen.

Die Hisbollah, die libanesische Regierung und das libanesische Militär sowie die Regierung, das Militär und wichtige Institutionen und Organisationen in der gesamten aufstrebenden multipolaren Welt müssen sich im Bereich der Informationstechnologie ebenso dringend selbst versorgen, wie sie es in anderen Bereichen der nationalen Sicherheit tun.

Die Herstellung von Computern, ihren einzelnen Komponenten, einschließlich Prozessoren, Smartphones, Funkgeräten, Pagern und allen anderen Geräten, sowie von Software und Online-Plattformen muss von einer Nation selbst oder einem vertrauenswürdigen Verbündeten entworfen, hergestellt und oder kodiert werden. Die Entwicklung, Herstellung und Programmierung von Hard- und Software, die im gesamten Informationsbereich eingesetzt wird, muss von Experten überwacht werden, die in den Regierungen, Organisationen und Institutionen arbeiten, die Informationstechnologie erwerben.

Hätte die Hisbollah IT-Hardware und -Software als zentral für ihre organisatorische Sicherheit und die nationale Sicherheit des Libanon eingestuft, hätte sie eine ganze Organisation geschaffen, die sich mit dem Erwerb, der Nutzung und der Gewährleistung der Sicherheit dieser Technologie befasst. Ihre Experten hätten die Produktion der Pager überwacht, mit denen sie ihre Smartphones ersetzen wollten, sie hätten deren Transport zu den Endnutzern überwacht, und die Möglichkeit, 5.000 Pager mit Sprengsätzen zu versehen, wäre unvorstellbar gewesen.

Mit anderen Worten: Der Kauf von IT-Hardware oder -Software sollte nicht als Erwerb harmloser Konsumgüter betrachtet werden, sondern als zentral für die nationale und betriebliche Sicherheit und unter der Annahme, dass potenzielle Feinde eine Gelegenheit zur Kompromittierung dieser wichtigen Technologie nutzen werden.

Es ist von zentraler Bedeutung, wie und von wem diese Güter entwickelt, hergestellt und versandt werden. Wenn ein Teil der Lieferkette diese Technologie in die Hände eines potenziellen Feindes bringt, sollte davon ausgegangen werden, dass gekaufte Geräte oder Software kompromittiert wurden.

Sicherung des Informationsbereichs in der multipolaren Welt

Während Nationen wie Russland und China in Bezug auf die Sicherung ihres Informationsraums sowie der dazugehörigen Hard- und Software den meisten weit voraus zu sein scheinen, ist dies bei vielen Verbündeten und potenziellen Verbündeten nicht der Fall. Die antiquierte Haltung gegenüber dem Informationsraum, der eher als Randbereich der nationalen Sicherheit betrachtet wird, hat zu einer tiefen Kultur der Selbstgefälligkeit, Ignoranz und Inkompetenz geführt.

Den USA, Israel und möglicherweise dem in Taiwan ansässigen Hersteller der Pager (oder ihren europäischen Partnern) ist es gelungen, diesen bösartigen, wahllosen Terroranschlag im Libanon auszuführen, und zwar nicht aufgrund besonderer Fähigkeiten ihrerseits und auch nicht aufgrund eines vorübergehenden Sicherheitsdefizits des Libanon, sondern weil der Informationsraum des Libanon praktisch ungeschützt bleibt, ohne dass man sich darüber im Klaren ist, dass er überhaupt geschützt werden sollte, geschweige denn, dass es eine wirksame Strategie dafür gibt.

Dieser Anschlag war vermeidbar. Künftige Angriffe sind vermeidbar.

So wie Russland und China traditionellere Foren und Übungen durchführen, die sich mit den traditionellen Bereichen der nationalen Verteidigung – Land, Luft und See – befassen, sind Foren und Übungen, die sich auf die Verteidigung des Informationsbereichs konzentrieren, unerlässlich. Wenn man Nationen, Regierungen, Verwaltungen, Organisationen, Institutionen und sogar Einzelpersonen davon überzeugt, wie wichtig es ist, die Souveränität über die Informationstechnologie zu behalten und diese Technologie entweder selbst herzustellen oder sie von engen Verbündeten zu erwerben,

die sie in einem transparenten Prozess von der Fabrikhalle über den Transit bis zur Verteilung selbst überwachen, wird das offene und unbewachte Tor, das die USA und ihre Stellvertreter bei diesem jüngsten Angriff ausnutzten, beseitigt.

Die Verteidigung nationaler Sicherheitsbereiche ist bereits eine gewaltige Aufgabe, wenn man sie richtig angeht. Der Informationsraum ist vielleicht der komplizierteste und am wenigsten verstandene Bereich in diesen Sphären. Aber in vielen Fällen ist der politischen und militärischen Führung nicht klar, dass der Informationsraum überhaupt ein nationaler Sicherheitsbereich ist. Eine Änderung dieser Einstellung und die Ausweitung der bestehenden gemeinsamen Verteidigungszusammenarbeit auf den Informationsraum ist der erste Schritt, um sicherzustellen, dass sich diese Tragödie – zumindest im Falle eines erneuten Versuchs – nicht so leicht wiederholen oder ein so großes Ausmaß annehmen wird.