Abwehr von Cyber-Attacken

Firmen wollen mehr Sicherheit

In einer Welt, in der nahezu alles digitalisiert und vernetzt ist, sind Angriffe auf Computersysteme gängige Praxis geworden – sowohl von Kriminellen als auch im Rahmen von militärischen Konflikten. Experten aus Luxemburg erklären, was es mit Cyberangriffen auf sich hat.

Text: Jeff Karier • Fotos: Gerry Huberty / Shutterstock

Seit dem Angriff Russlands auf die Ukraine hört man immer wieder Schlagworte wie Cyberwarfare, also digitale Kriegsführung. Wobei der Begriff laut Professor Gabriele Lenzini vom Interdisciplinary Centre for Security, Reliability and Trust (SnT) an der Universität Luxemburg oft sehr frei verwendet wird. „Nicht jede Cyberattacke, die sich gegen ein Land richtet oder im Namen eines Landes durchgeführt wird, kann als Cyberwarfare bezeichnet werden“, betont der Computerwissenschaftler. Auch wenn es keine allgemeingültige Definition für Cyberwarfare gibt, bezieht er sich auf das sogenannte Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Dieses definiert etwa Cyberwaffen als Mittel der Cyber-Kriegsführung, „die eingesetzt werden, konzipiert sind oder eingesetzt werden sollen, um Personen zu verletzen oder zu töten oder Objekte zu beschädigen oder zu zerstören.“ Das heißt, dass sowohl Ziel als auch Konsequenz einer militärischen Cyberattacke Schaden an Mensch und/oder Material sind.

„Zum Cyberwarfare gehören Angriffe, die Unterwanderung und die Störung kritischer Infrastruktur. Dies geschieht oft mittels sogenannter DDoS-Attacken (siehe Kasten, Anm. d. Red.), welche IT-Infrastrukturen überlasten“, heißt es auf Anfrage vom Chaos Computer Club Lëtzebuerg (C3L), dem hiesigen Ableger der größten europäischen Hackervereinigung. Zu den bevorzugten Zielen in der Cyber-Kriegsführung gehören somit neben beispielsweise Kraftwerken oder der Wasserversorgung auch Ziele, durch die man die Verteidigungsfähigkeit der Gegenseite schwächt oder sich einen militärischen Vorteil verschafft. „Dazu zählen auch Satelliten. Sie sollten entsprechend gut abgesichert oder verteidigt werden. Schließlich fußen viele moderne Waffensysteme auf Satellitendaten“, erklärt Professor Marcus Völp, der am SnT an der Universität Luxemburg unter anderem zu resilienten und belastbaren Computersystemen forscht. Fallen Satelliten aus, können diese Waffensysteme nicht oder nur noch eingeschränkt genutzt werden.

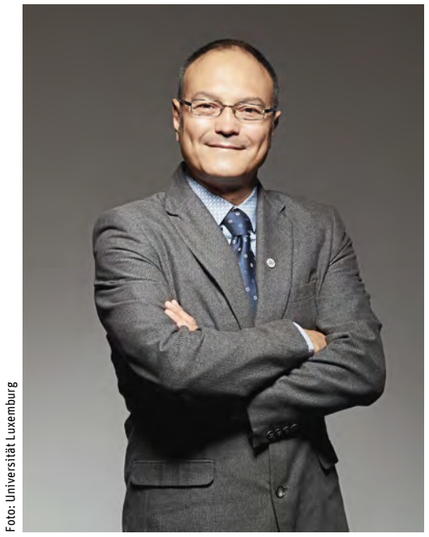

Foto: Universität Luxemburg

„Cyber-Attacken sind nicht so unmittelbar wie etwa die Bombardierung eines Ziels.“

Professor Gabriele Lenzini vom Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg, über den Charakter von Cyberattacken

Hybride Kriegsführung

Weitere Beispiele von Cyberangriffen der letzten Jahre sind laut Chaos Computer Club Lëtzebuerg etwa der Triton-Malware-Angriff auf ein saudisches Petrochemie-Werk. „Die Schadsoftware wurde mit der Intention geschrieben, dass das Werk explodiert oder zumindest giftige Gase austreten. Also mit der vollen Absicht, Menschenleben in Gefahr zu bringen.“ Aber auch ein Angriff auf das israelische Wassersystem Mitte 2020 zählen zu derartigen digitalen Attacken. „Hier wollte man die Chlor-Werte des Wassers auf ein giftiges Niveau bringen, um die Wasserversorgung zu stören. Dies während einer Wasserknappheit durch eine Hitzewelle und während des Covid-19-Ausbruchs.“ Solche Attacken können laut Marcus Völp jedoch je nach Definition auch als Cyberterrorismus angesehen werden. So oder so zeigen diese Angriffe die Gefahr, die von ihnen ausgeht.

Digitale Attacken werden immer häufiger nicht isoliert, sondern in einer strategischen Kombination mit konventioneller Kriegsführung eingesetzt. Wie eine solche hybride Kriegsführung aussehen kann, sieht man aktuell in der Ukraine. Kurz bevor Russland in den Nachbarstaat einmarschierte, führten allem Anschein nach Hacker im Auftrag Russlands einen digitalen Erstschlag aus.

Laut dem Sicherheitsunternehmen Sentinel One wurde am Tag der russischen Attacke am 24. Februar eine russische Wiper-Software eingesetzt. Diese löscht und zerstört Daten. Die Satelliten-Modems des US-amerikanischen Netzbetreibers Viasat in der Ukraine wurden so funktionsunfähig gemacht. Ziel sei es gewesen, die Kommunikation der ukrainischen Verteidigungskräfte zu stören. Es gab aber auch Kollateralschäden. Denn auch die Modems in 5800 satellitengestützten Windrädern in Europa wurden durch den Angriff irreparabel beschädigt.

„Die Grenzen zwischen kriminellen Cyber-Angriffen, die zum Ziel haben, Geld oder Informationen zu erbeuten, und kriegerischen beziehungsweise militärischen Cyberattacken, die Schaden anrichten sollen, sind recht fließend. Schließlich können bei beiden Arten von Angriffen dieselben Mechanismen, Einfallstore und Werkzeuge genutzt werden“, erläutert Völp. Sollen spezifische Systeme attackiert werden, folgen Hacker in der Regel einem gewissen Ablauf. „Zunächst werden die Systeme observiert, es werden also Informationen gesammelt. Etwa, wer Zugriff auf dieses System hat. Denn Menschen sind oft der einfachste Zugangspunkt.“ Das kann etwa über das Versenden von Phishing-Mails erfolgen. Das passiert immer wieder, nicht zuletzt, weil Kriminelle immer raffinierter beim Fälschen von Mails werden.

Systeme verfügen oft über noch nicht bekannte Sicherheitslücken. Diese werden als Zero-Day, also Tag-Null, bezeichnet. Diese sind besonders für den Cyber-Krieg von großer Bedeutung, da über solche Angriffspunkte auch der Zugriff zu kritischen Systemen gelingen kann. Entsprechend werden Informationen zu solchen Zero-Day-Schwachstellen im Darknet für hohe Summen gehandelt.

Systeme verfügen oft über noch nicht bekannte Sicherheitslücken. Diese werden als Zero-Day, also Tag-Null, bezeichnet. Diese sind besonders für den Cyber-Krieg von großer Bedeutung, da über solche Angriffspunkte auch der Zugriff zu kritischen Systemen gelingen kann.

„Bevorzugte Ziele sind zwar weiterhin Finanzinstitute, aber auch jene Unternehmen, die wirtschaftlich sehr gut dastehen.“

Pascal Steichen, Geschäftsführer von Security Made in Lëtzebuerg (Smile), über die Vorgehensweise von Kriminellen

„Seit einigen Jahren haben große Unternehmen wie zum Beispiel Microsoft, Google und Meta Kopfgeld-Programme. Personen, die Sicherheitslücken in ihrer Software gefunden und ihnen verantwortungsbewusst mitgeteilt haben, erhalten ein Preisgeld sowie Anerkennung. Das können mehrere Hunderttausend Euro sein“, hebt Gabriele Lenzini hervor. Geheimdienste sowie Sicherheitsorgane verschiedener Staaten haben ähnliche Wettbewerbe ins Leben gerufen, um neue Talente für ihre Cyberabwehr-Einheiten zu gewinnen.

„Cyber-Attacken sind nicht so unmittelbar wie etwa die Bombardierung eines Ziels. Die Konsequenzen können zeitverzögert sein oder sich über einen längeren Zeitraum erstrecken“, betont er. Opfer von Cyberattacken jeglicher Art wissen somit nicht nur lange Zeit nicht, dass sie Opfer sind, sie wissen auch nicht, was das Endziel ist, ob also die Angreifer nicht noch mehr geplant haben, als etwa nur Daten zu entwenden. „Meistens sind wir es, die die Unternehmen und Gemeinden kontaktieren, weil festgestellt wurde, dass eine IP, die zu ihnen gehört, bei einer Attacke zu den Zielen gehörte“, erklärt Pascal Steichen, der Geschäftsführer von Security Made in Lëtzebuerg (Smile), eine Cybersicherheits-Agentur für die Luxemburger Wirtschaft und Gemeinden. Zu deren Aufgabenbereichen gehört es unter anderem, Privatunternehmen und Gemeinden im Falle eines Angriffs zu helfen.

Daten als Geisel

Die Priorität der Computer Emergency Response Teams, der Notfallteams von Smile, ist es herauszufinden, wie die Angreifer eingedrungen sind, welche Systeme kompromittiert wurden und welche Auswirkungen der Angriff hat. Wurden etwa Daten entwendet, zerstört oder verschlüsselt? Letzteres geschieht durch Ransomware. Der Hacker nimmt die Daten als Geisel und verlangt ein Lösegeld, um diese wieder zu entschlüsseln. Laut einer Analyse des US-IT-Unternehmens Parachute verursachte Ransomware 2021 weltweit einen wirtschaftlichen Schaden in Höhe von rund 20 Milliarden US-Dollar (18,36 Milliarden Euro).

Wie Steichen erklärt, seien alle Branchen von solchen Angriffen betroffen, da die Angreifer mit der Gießkanne sehr breit gestreut versuchen, in Systeme einzudringen. „Bevorzugte Ziele sind zwar weiterhin Finanzinstitute, aber auch jene Unternehmen, die wirtschaftlich sehr gut dastehen, da Kriminelle davon ausgehen, dass diese im Falle von Ransomware auch imstande sind, das Lösegeld zu zahlen." Das zeige, dass zu Hackergruppen auch Personen mit Wirtschaftskenntnissen gehören.

Wachsender Sektor

Aber nicht alle Unternehmen können eine solche Attacke verkraften. „Einige Unternehmen sind nach einer Ransomware-Attacke pleite gegangen, weil sie sich nicht mehr erholt haben. Egal, ob sie das Lösegeld gezahlt haben oder nicht", hebt Lenzini hervor.

Die Gefahr wird von der Wirtschaft ernst genommen. „Immer mehr Unternehmen sind sich der Wichtigkeit der Absicherung ihrer Systeme gegenüber Angriffen bewusst. Wenn man die letzten rund sechs Jahre betrachtet, steigt die Zahl an Firmen, die auf uns zukommen, immer weiter an", erklärt Steichen. So seien auch die Fähigkeiten der Unternehmen, Angriffe zu entdecken und zu reagieren, besser geworden. Insgesamt sei der Sektor der Cyber-Sicherheit in Luxemburg stark gewachsen. So

Foto: Universität Luxemburg

„Heutige Systeme sind so groß, dass es unmöglich ist, alle Schwachpunkte zu vermeiden."

Professor Marcus Völp vom Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg, über die Unvermeidbarkeit von Schwachpunkten

habe sich in den letzten Jahren die Zahl der Cyber-Sicherheitsunternehmen hierzulande verdoppelt.

Aber auch die Universität baut ihre Kompetenzen im Bereich Cyber kontinuierlich aus. So wurde am 20. April bekannt gegeben, dass ein Lehrstuhl für Cyber-Politik im September 2022 eingerichtet wird. Dieser soll sich mit den rechtlichen und politischen Aspekten an der Schnittstelle von digitalen und Netzwerktechnologien beschäftigen. Dazu gehören auch Cyber-Kriminalität sowie Cyber-Verteidigung.

Wenn es zu einem Cyberangriff kommt, der von einem Angriffserkennungssystem erkannt wird, können Notfalleinsatzteams je nach Art der Attacke etwa versuchen, das System so schnell wie möglich herunterzufahren, um Schaden abzuwenden. „Bei anderen Attacken stellt das Notfalleinsatzteam dem System weitere Kapazitäten zur Verfügung, um eine Überlastung zu verhindern oder es leitet Datenverkehr um, um so den Angriff ins Leere laufen zu lassen", erklärt Lenzini.

Viren und andere Programme verschwinden nach dem Angriff nicht. Sie können analysiert werden, um etwa deren Herkunft zu ermitteln. Allerdings heißt das nicht, dass man dadurch auch nachweisen kann, wer der Angreifer ist. „Die Werkzeuge, um Cyberangriffe auszuführen, sind im Netz und können theoretisch von jedem genutzt werden", betont Marcus Völp. Man kann zwar versuchen, den Internetverkehr zurückzuverfolgen. Da Hacker aber oft Systeme nutzen, die sie zuvor ohne Wissen ihrer Nutzer infiziert haben, um anzugreifen, oder über andere Wege den Ursprung der Attacke verschleiern, führt die Spurensuche oft ins Nichts.

„Heutige Systeme sind so groß, dass es unmöglich ist, alle Schwachpunkte zu vermeiden", unterstreicht der Experte. Das sieht Pascal Steichen von Smile ähnlich, der betont, dass aufgrund der Vernetzung und Digitalisierung die Angriffsfläche für Hacker sehr groß geworden ist. Und der Chaos Computer Club Lëtzebuerg erklärt: „Heutzutage ist beinahe alles miteinander vernetzt oder wird ‚smart'. Dabei ist smart leider meistens eher ein Euphemismus für ‚angreifbar'."

Resiliente Systeme schaffen

Daher betonen die beiden Forscher Marcus Völp und Gabriele Lenzini, wie wichtig es ist, Systeme so zu konzipieren, dass sie Attacken aushalten können. Hier spricht man von resilienten und belastbaren Systemen. „Sie sollen Attacken standhalten oder ausreichend lange tolerieren können, bis etwa automatische Reparatursysteme greifen oder, wenn diese nicht ausreichen, Menschen aktiv werden und entsprechende Gegenmaßnahmen einleiten können", präzisiert Völp. So könnten Systeme etwa wie diejenigen in Flugzeugen auf mehrere Computer aufgeteilt werden. Fällt ein Computer aus, kann das System trotzdem weiterhin funktionieren. Die beiden Forscher wollen hierbei in Zukunft noch enger mit der Privatwirtschaft zusammenarbeiten. Hierzu Völp: „Gemeinsam mit den Unternehmen können wir an Lösungen forschen und neue Strategien oder Technologien für die Zukunft entwickeln."

DDoS Attacken
Bei einem Distributed-Denial-of-Service (DDoS)-Angriff wird ein Dienst wie etwa eine Website durch massive Anfragen überlastet, sodass dieser nicht mehr oder nur noch stark eingeschränkt erreichbar ist.

Botnets
Dabei handelt es sich um ein Netzwerk von Geräten, die von Hackern mit Schadsoftware infiziert wurden. Diese Bots agieren von da an unauffällig im Hintergrund, ohne dass die Nutzer etwas davon bemerken.

Phishing
Der Versand gefälschter E-Mails, die Menschen dazu verleiten sollen, auf Links zu klicken oder einen Anhang herunterzuladen. So sollen Nutzer sensible Daten preisgeben oder es wird Schadsoftware in das System des Nutzers eingespeist.