Chinesische Hacker greifen USA über Kuh-App an | *bluewin.ch*

Datenschutz bei Marketing und Werbung – Das ist zu beachten | *dr-datenschutz.de*

BNP Paribas bars Russia-based staff from computer systems as cyber attack fears grow | *reuters.com*

Analysen & Hintergründe

CYBERKRIEG (CYBERWAR)

Cyberangriffe: Gezielte Attacken und Grundrauschen

Warnungen und Befürchtungen davor, dass Deutschland aufgrund der Weltlage in einen Cyberkrieg gezogen werden kann, finden sich nicht nur in den Medien. Auch Behörden und Politik warnen vor Aktivitäten staatlicher russischer Akteure gegen Ziele in Wirtschaft und Verwaltung. Eine Einordnung der Bedrohung.

Jens Ohlig

Droht Deutschland ein Cyberwar? Am Rande Europas verschärft sich die „Cyberlage“ schon seit Anfang des Jahres. Regierungswebseiten wurden übernommen und mit Nachrichten wie „Habt Angst und rechnet mit dem Schlimmsten“ versehen, Daten unwiderruflich gelöscht (Tagesspiegel Background berichtete). Mit Beginn des militärischen Überfalls Russlands auf die Ukraine folgten flankierende DDoS-Attacken (Tagesspiegel Background berichtete). **Aggression und Aktivität im Cyberraum** sind unbestreitbar hoch, aber ist das schon der Krieg der Zukunft, bei dem der Konflikt digital geführt wird?

Und wie hoch ist die Gefahr für **deutsche Unternehmen und staatliche Institutionen**?

Vergleich von Cyberangriffen und Krieg schwierig

Sehr hoch, warnen Sicherheitsbehörden wie das **Bundesamt für Verfassungsschutz** (BfV) oder das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) seit Wochen. Es seien Angriffe auf „Hochwertziele“ in Deutschland in Vorbereitung, meldete der „Spiegel“ kürzlich mit Verweis auf einen entsprechenden Lagebericht des BSI.

Thorsten Holz, Leiter der Forschungsgruppe zu systemnaher IT-Sicherheitsforschung am **Helmholtz-Zentrum für Informationssicherheit** (CISPA) verweist allerdings im Hinblick auf die Cyberbedrohungslage in Deutschland auf die Situation vor Ort: „Momentan gibt es vor allem die konventionellen Angriffe in der Ukraine und dort sterben Menschen, der Vergleich zu Cyberangriffen ist also schwierig.“ Gezielte Angriffe auf Deutschland würden „eine deutliche Eskalation bewirken“, so Holz.

Jörn Müller-Quade vom **Institut für Informationssicherheit und Verlässlichkeit des Karlsruher Instituts für Technologie** (KIT) verweist zwar darauf, dass Firmen, öffentliche Einrichtungen und Institutionen auf digitale Bedrohungen der Kritischen Infrastruktur ungenügend vorbereitet seien. Der ganz große Angriff im Cyberkrieg könnte dennoch ausbleiben, glaubt er. „**Der große Knall ist nicht immer das Ziel**, insbesondere weil dieser sofort bemerkt wird und Gegenmaßnahmen auslöst.“ Tatsächlich liefen **viele Angriffe im Hintergrund**, etwa um Ziele ausspähen, um später größere Attacken vorzubereiten.

Was hat Russland von einer offenen Cyberattacke gegen einen Nato-Staat?

Mit den Sanktionen gegen Russland sowie zahlreichen

Waffenlieferungen von EU-Staaten an die Ukraine hätte Putin womöglich genug Gründe, über einen **elektronischen Vergeltungsschlag auf Nato-Länder** nachzudenken. Doch Expert:innen gehen nicht von offenen militärischen Cyberoperationen aus und ordnen die Lage differenzierter ein: „Ich denke die Warnungen des BSI und des BfV sollten in jedem Fall **ernst genommen** werden. Insbesondere im Cyberspace ist die Lage aktuell sehr unübersichtlich. Ich glaube zwar weiterhin, dass Russland davon absehen wird, mit offiziellen militärischen oder nachrichtendienstlichen Kräften IT-Systeme in Europa und Deutschland anzugreifen, **da es Russland keine Vorteile verschaffen würde**“, sagt **Thomas Reinhold**, Wissenschaftlicher Mitarbeiter am Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (**PEASEC**) der **TU Darmstadt**.

Allerdings gebe es neben den staatlichen Akteuren auch **nichtstaatliche Gruppen** aus dem Bereich Cyberkriminalität oder Hacker:innenkollektive, die in ihrem Handeln schwieriger einzuschätzen seien: „Gerade **Gruppen, die sich der Sache Russlands verschrieben haben**, könnten IT-Angriffe als Vergeltungsmaßnahmen für die Sanktionen durchführen — die aus Sicht Putins ja als völlig ungerechtfertigt dargestellt und die in keine Relation zu dem Krieg gesetzt werden.“

Matthias Schulze, stellvertretender Forschungsgruppenleiter Sicherheitspolitik der Stiftung Wissenschaft und Politik (**SWP**) sieht die Gefahr ebenfalls in aktivistischen Ad-Hoc-Aktionen: „Ich halte es für wahrscheinlich, dass wir demnächst mehr – vermutlich durch russische oder von pro-russischen **Hacktivisten** gestartete – **Cyberoperationen in Deutschland** sehen werden.“ Vieles spräche dafür, dass Russland von der scharfen Reaktion des Westens überrascht worden sei und demnach auch nicht so viel Zeit für gesonderte Vorbereitungen von neuen Cyberoperationen gegenüber der EU hatte.

Schulze denkt dabei allerdings an keinen Cyberangriff mit **Blackout** in Deutschland: „Ob bei uns aber die Lichter ausgehen ist eine andere Frage, da das schwer und **nur mit viel Aufwand und zeitlichem Vorlauf** zu bewerkstelligen wäre – viele Monate bis Jahre." Für wahrscheinlicher hält er **niedrigschwellige Operationen** wie Hacking gegen Politiker:innen mit dem anschließendem Leaking der erbeuteten Informationen. Auch **Desinformationssoperationen** zum Schüren von **Ressentiments gegen ukrainische Geflüchtete** oder den **Kurs der Regierung** seien denkbar. Solche Operationen verfolgten das Ziel, den gesellschaftlichen Rückhalt für die Maßnahmen des Westens zu schwächen. Das entspräche mehr dem Modus Operandi Russlands.

Klar ist: Russland operiert militärisch mit Cyberangriffen. Einige der Gruppen, denen Angriffe eindeutig zugeordnet werden können, sind direkt als Einheiten dem **militärischen Geheimdienst GRU** unterstellt, wie die als „**Sandworm**" bekannt gewordene Einheit 74455. Der Cyberraum ist also mittlerweile kein ziviler Raum mehr, in dem es Konsens unter den Staaten ist, dass er im Interesse aller Menschen zu schützen ist — längst wird er auch als Operationsgebiet mitgedacht, um Interessen durchzusetzen.

Wenn das Bundesamt für Verfassungsschutz davor warnt, dass die staatlich gelenkte russische Gruppe „**Ghostwriter**" wieder mit Aktivitäten in Deutschland sichtbar wird, ist das eine konkrete Bedrohung und kein Geraune. Die Gruppe, der Phishing-Attacken im März vergangenen Jahres gegen sieben Bundestagsabgeordnete und mehr als 70 Landtagsabgeordnete zugeordnet werden, hat in den letzten Tagen eine **erneute Phishing-Kampagne** gestartet.

Trotz der erhöhten Gefährdungslage, die Behörden in Deutschland aufgrund des Kriegs in der Ukraine annehmen, unterscheidet sich die Warnung des Verfassungsschutzes aber **nicht grundsätzlich von**

Warnungen zu anderen Cybersicherheitsvorfällen — Angriffe auf IT-Systeme finden auch außerhalb kriegerischer Konflikte beständig statt, wenn nicht militärisch motiviert, dann als Ransomware mit krimineller finanzieller Motivation. Der **Schutz gegen Risiken und die Abwehr von Angriffen** ist ein Prozess und muss auch außerhalb von weltpolitischen Krisen ein ständiger Teil der Sicherheitsarchitektur in Wirtschaft und Verwaltung sein.

Die Warnungen des BSI greift deshalb auch der Branchenverband **Bitkom** auf. Dessen Präsident **Achim Berg** forderte alle Unternehmen auf, unbedingt ihren Schutz vor Cyberangriffen zu prüfen und wo nötig zu verstärken. „Es ist kein Geheimnis, dass Russland und mit staatlichen Stellen verbundene Gruppierungen über entsprechende Fähigkeiten verfügen“, sagte Berg. Acht von zehn Digitalunternehmen (**84 Prozen**t) gaben bei einer aktuellen Umfrage des Digitalverbandes an, dass sie von einer **verschärften Bedrohungslage im Cyberraum** ausgehen würden. Zwei Drittel (67 Prozent) der Unternehmen erwarteten dies für die Zukunft, weitere 17 Prozent sähen bereits aktuell konkrete Anzeichen dafür. Gleichzeitig hätten laut der nicht repräsentativen Umfrage zufolge nun jedes dritte Unternehmen (34 Prozent) seine IT-Schutzmaßnahmen **kurzfristig hochgefahren**.

Cyberangriffe als „Grundrauschen“ der IT-Sicherheit und als begleitende Nadelstiche im Krieg sind Teil der Wirklichkeit im Cyberraum des Jahres 2022. Ein gezielter Angriff auf Nato-Länder mit dem **Ausfall der Stromversorgung** ist für Russland allerdings mit ganz drastischen Konsequenzen verbunden, so Thomas Reinhold bereits Ende Februar auf Nachfrage von Tagesspiegel Background: „Dies könnte ganz am Ende auch dazu führen, dass Artikel 5 der Nato-Charta ausgelöst wird.“ Und das würde den Kriegseintritt des Nato-Bündnisses bedeuten.