BDI

INFORMATION | RUSSLAND-KONFLIKT | ARBEITSPAPIER

Cybersicherheit

Aktuelles. Risiken. Handlungsoptionen.

24. März 2022

Aktuelles

- Neben den russischen Angriffen zu Land, Luft und Wasser verzeichnet die Ukraine seit Mitte Februar 2022 eine hohe Anzahl an Distributed-Denial-of-Service- sowie Ransomware-Angriffen auf Regierungsinstitutionen und Banken.
- **Cyberangriffe / Hacktivism:** Im Kontext des völkerrechtswidrigen Angriffs Russlands auf die Ukraine ist es in Deutschland bisher nur zu sehr wenigen, nicht zusammenhängenden Cyberangriffen gekommen. Durch den Ausfall des Satellitennetzwerks KA-SAT wurden Ende Februar die Fernwartungszugänge zu ca. 5.000 Windkraftanlagen in Deutschland unterbrochen. Die Energieerzeugung blieb davon unberührt. Am 12. März 2022 haben Aktivistinnen und Aktivisten von Anonymous die deutsche Niederlassung eines russischen Energiekonzerns angegriffen. Dabei wurden nach Medienangaben 20 Terabyte an Daten erbeutet. Eine Auswirkung auf die Energieversorgung gab es nach unseren Erkenntnissen nicht. Das Hackerkollektiv Anonymous ruft seit einigen Tagen über den Kurznachrichtendienst Twitter direkt einzelne westliche Unternehmen zum Rückzug aus Russland auf. Es droht westlichen Unternehmen, die dieser Aufforderung nicht nachkommen, dass sie Ziel von Hacktivism-Maßnahmen von Anonymous werden könnten.
- **Einsatz russischer Antivirensoftware:** Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt seit dem 15. März 2022 vor dem Einsatz einer russischen Antivirensoftware: „*Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt nach §7 BSI-Gesetz vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen*.“
- **Desinformationen:** Russland nutzt neben der Propaganda im eigenen Land auch weiterhin insbesondere Soziale Medien zur Verbreitung von Desinformationen, die auf Personen in der Ukraine sowie im Westen abzielen, zugleich wurden in Russland zahlreiche westliche Soziale Medien als „extremistisch“ eingestuft. In Europa besteht die Gefahr von Fake News im Kontext des Flüchtlingszustroms aus der Ukraine. Auch werden zunehmend über einzelne russische Botschaften Desinformationen zu vermeintlichen Angriffen auf russische Staatsangehörige in Europa verbreitet.
- **Schadsoftware:** Zu Beginn des völkerrechtswidrigen Angriffs Russlands auf die Ukraine wurde die Schadsoftware *Hermetic Wiper* gezielt in der Ukraine verbreitet, ab dem 15. März 2022 dann zusätzlich die Schadsoftware „CaddyWiper“. Während bei Ransomware-Angriffen Daten auf Computern verschlüsselt werden, kommt es bei einem Wiper-Angriff zu einer Zerstörung / Löschung der Dateien – teilweise ist das Endgerät anschließend unbrauchbar.

Steven Heckler | Digitalisierung und Innovation | T: +49 30 2028-1523 | s.heckler@bdi.eu | www.bdi.eu

- **Maßnahmen auf europäischer Ebene:** Der Europäische Rat fordert am 9. März 2022 die EU-Kommission zur Etablierung eines Emergency Response Funds for Cybersecurity auf. Durch den Fonds, dessen Höhe nicht spezifiziert wurde, soll der Ausbau der Cybersicherheitskapazitäten der Mitgliedsstaaten unterstützt werden.

Risiken

Allgemein

- Der Hacktivism von nichstaatlichen Gruppierungen in Russland, der Ukraine sowie Europas könnte zu unbeabsichtigten, jedoch potenziell weitreichenden Folgen (Spillover-Effekte) und damit ggfls. zu einer Eskalation der Sicherheitslage führen.

Für die Ukraine

- Analog zum Cyberangriff auf einen ukrainischen Stromversorger im Dezember 2015 durch den etwa 230.000 Kunden in der Westukraine ohne Strom waren, könnten russische Cyberkriminelle zur Destabilisierung der Lage in der Ukraine noch weitreichendere Cyberangriffe als in den letzten Tagen durchführen.

Für die deutsche Industrie

- BSI-Einschätzung: Das BSI sieht eine „abstrakt erhöhte Bedrohungslage für Deutschland“. Dem BSI ist jedoch „keine akute unmittelbare Gefährdung der Informationssicherheit in Deutschland im Zusammenhang mit der Situation in der Ukraine ersichtlich“. Auch werden in Deutschland bis dato nicht vermehrt Cyberangriffe registriert.
- Weiterhin wird vor Phishing-Mails im Kontext des Russland-Ukraine-Kriegs (z. B. bezugnehmend auf das geltende wirtschaftliche Sanktionsregime oder Spendenaufrufe) gewarnt.
- Deutsche Unternehmen sollten insbesondere Schutzmaßnahmen von Standorten in der Ukraine und in Russland soweit wie möglich erhöhen und diese – sofern möglich – von der restlichen Konzern-IT trennen. Durch die weltweite Vernetzung von IT-Systemen kann es zu Schäden in Folge von Cyberangriffen kommen.
- Sollte es in Folge des russischen Enteignungsgesetzes zur Enteignung von deutschen Unternehmen in Russland kommen, bestünde die Gefahr, dass russische Akteure Zugriff auf die Unternehmens-IT deutscher Unternehmen bekommen. Die daraus resultierenden Folgen für die IT-Sicherheit in Deutschland lassen sich nicht abschließend abschätzen und können einzelfallspezifisch sehr hoch sein.

Handlungsoptionen

Kurzfristig

- Unternehmen und staatliche Einrichtungen in Deutschland sollten weiterhin ihre IT- und OT-Systeme kontinuierlich überwachen und durch geeignete Maßnahmen entsprechend der Empfehlungen der Allianz für Cybersicherheit härten.
- Unternehmen, die in Russland Produktionsstätten sowie IT-Infrastrukturen haben, sollten vor dem Hintergrund des russischen Enteignungsgesetzes Maßnahmen vorbereiten, um ihre IT-Infrastrukturen zwischen Russland und Europa trennen zu können.

- Mitglieder der Allianz für Cybersicherheit können täglich einen Sonderbericht des BSI zu aktuellen Cyberbedrohungen im Kontext des Russland-Ukraine-Kriegs abrufen. Eine Mitgliedschaft in der ACS ist kostenfrei.

Mittelfristig

- Es ist zu begrüßen, dass sich die Telekommunikationsminister am 9. März 2022 in Nevers darauf verständigt haben, dass der NIS 2-Gesetzgebungsprozess rasch abgeschlossen werden soll. Da die NIS 2 nach Abschluss des Trilogverfahrens erst noch innerhalb von 18 bis 24 Monaten in nationales Recht umgesetzt werden muss, ist zu erwarten, dass sie kurzfristig keinen Beitrag zur Stärkung der Cyberresilienz Europas leisten wird. Ferner sieht die deutsche Industrie weitreichenden Anpassungsbedarf am vorliegenden Gesetzentwurf. Die Bundesregierung sollte sich für eine NIS 2-Richtlinie einsetzen, die dem notwendigen risikobasierten Ansatz Rechnung trägt und möglichst wenig Bürokratie entstehen lässt. Ferner sollten auch staatliche Einrichtungen der Kommunal- und Landesebene in den Anwendungsbereich der Richtlinie fallen.

Langfristig

- Vor dem Hintergrund der hybriden Kriegsführung sollten auch die Cyberfähigkeiten und DIgitalkompetenzen der Bundeswehr im Rahmen des Sondervermögens (100 Milliarden Euro) gestärkt werden.
- Die EU-Kommission hat am 16. März 2022 die Konsultation zum EU Cyber Resilience Act begonnen. Dieser Rechtsakt zielt auf die Einführung horizontaler Cybersicherheitsanforderungen ab. Produkte und Dienstleistungen, die ein risikoadäquates Cybersicherheitsniveau gewährleisten, sind ein wichtiger Baustein zur Stärkung der Cyberresilienz Europas. Die Bundesregierung sollte sich daher weiterhin für eine rasche Entwicklung eines entsprechenden EU-Rechtsakts einsetzen.