BDI

INFORMATION | RUSSLAND-UKRAINE-KRIEG | ARBEITSPAPIER

Cybersicherheit

Aktuelles. Risiken. Handlungsoptionen.

13. Mai 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, Banken sowie Betreiber Kritischer Infrastrukturen.

- **Cyberangriffe / Hacktivism:**
  - **Ukraine:**
    - Das ukrainische CERT warnt Organisationen in der Ukraine vor dem vermehrten Aufkommen des JesterStealer, ein Schadprogramm welches Anmeldedaten, Cookies und Kreditkartendaten vom angegriffenen Gerät sammelt und diese an den Angreifer sendet. Ferner weist das CERT-UA auf angeblich im Namen des CERT-UA versandte Mails hin, die das Schadprogramm CredoMap_v2 enthalten.
    - Über die seit Kriegsbeginn erfolgten Cyberangriffe auf die Ukraine informiert ein unlängst veröffentlichter Sonderbericht. Demnach zielten mehr als 40 Prozent der russischen Cyberangriffe auf Organisationen der Kritischen Infrastrukturen und ca. ein Drittel auf nationale, regionale und kommunale Regierungseinrichtungen.
    - Um ein besseres Lagebild über aktuelle Angriffsvektoren und Schwachstellen zu erhalten, bittet das ukrainische CERT um das Teilen von Informationen. Hierfür hat das CERT-UA die Website CERT-UA MISP online gestellt.
  - **Deutschland:**
    - Am 7. und 8. Mai haben russische Hacktivistinnen und Hacktivisten die Erreichbarkeit u.a der Webseiten des Bundesverteidigungsministeriums, des Bundestags und der Bundespolizei durch DDoS-Angriffe gestört. gekommen.
    - Durch den Ausfall des Satellitennetzwerks KA-SAT Ende Februar wurden die Fernwartungszugänge zu ca. 5.000 Windkraftanlagen in Deutschland unterbrochen und Anonymous hat Mitte März die deutsche Niederlassung eines russischen Energiekonzerns angegriffen. Die Energieerzeugung blieb davon jeweils unberührt.
  - **Global:** Das Hackerkollektiv Anonymous ruft weiterhin über Twitter westliche Unternehmen zum Rückzug aus Russland auf. Es droht 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 der Antivirensoftware von Kaspersky und empfiehlt die Virenschutzsoftware von Kaspersky durch alternative Produkte zu ersetzen.

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

- **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. In Europa besteht die Gefahr von Fake News im Kontext des Krieges.
- **Schadsoftware:** Zu Kriegsbeginn wurden die Satelliten-Modems des US-amerikanischen Netzbetreibers Viasat in der Ukraine durch den Wiper „Acid Rain“ (auch UKROP genannt) angegriffen. Daneben wurden seit Beginn des Krieges die Schadsoftware „Hermetic Wiper“, „WhisperKill“, „WhisperGate“, IsaacWiper, „CaddyWiper“ und DoubleZero gezielt in der Ukraine verbreitet. Ein Wiper-Angriff zerstört / löscht Dateien – teilweise ist das Endgerät anschließend unbrauchbar.

Risiken

Allgemein

- Der Hacktivism von nichtstaatlichen 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

- Es besteht die Gefahr, dass russische Cyberkriminelle zur weiteren 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“. Trotzdem ruft das BSI zur „erhöhten Wachsamkeit und Reaktionsbereitschaft auf.“

- 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. Ferner besteht die Gefahr des unrechtmäßigen Zugriffs auf das Geistige Eigentum westlicher Firmen in Russland durch russische staatliche Stellen sowie Cyberkriminelle.

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. Eine Mitgliedschaft in der ACS ist kostenfrei.

Langfristig

- Vor dem Hintergrund der hybriden Kriegsführung sollten auch die Cyberfähigkeiten und Digitalkompetenzen der Bundeswehr im Rahmen des Sondervermögens gestärkt werden.