BDI

INFORMATION | RUSSLAND-UKRAINE-KRIEG | ARBEITSPAPIER

Cybersicherheit

Aktuelles. Risiken. Handlungsoptionen.

7. September 2022

Aktuelles

- Neben den russischen Angriffen zu Land, Luft und Wasser verzeichnet die Ukraine auch weiterhin eine Vielzahl an Cybersicherheitsangriffen – insbesondere Distributed-Denial-of-Service- sowie Ransomware-Angriffe und Fälle von Online-Betrug – auf Regierungsinstitutionen, Banken, Betreiber Kritischer Infrastrukturen sowie weitere Organisationen in der Ukraine.
- **Spionage:** Der Militärische Abschirmdienst (MAD) warnt vor der zunehmenden Gefahr der Spionage aus Russland. „Insbesondere durch die Ausbildung ukrainischer Streitkräfte hier in Deutschland, aber auch durch die Waffenlieferungen in die Ukraine ist das Interesse an Deutschland als Drehscheibe noch einmal größer geworden“, so MAD-Präsidentin Martina Rosenberg. Neben der Ausbildung ukrainischer Streitkräfte stehe auch die Logistik im Fokus russischer Spionageaktivitäten in Deutschland. Die Bedrohungslage habe sich zuletzt erneut verschärft.
- **Cyberangriffe / Hacktivism:**
  - **Ukraine:**
    - Das ukrainische Computer Emergency Response Team (CERT-UA) hat Ende August die massive Verbreitung der AgentTesla-Malware verzeichnet. Am 30. und 31. August 2022 registrierte das CERT-UA den massenhaften Versand von E-Mails mit dem Betreff „Technische Zeichnung“ an ukrainische, österreichische und deutsche Organisationen. Der Anhang der E-Mail ist eine IMG-Datei, deren Öffnen zur Ausführung von Schadcode führt.
    - Das CERT-UA hat einen Anstieg der Zahl betrügerischer Seiten im sozialen Netzwerk Facebook festgestellt. Der Inhalt der Anzeigen auf solchen Seiten bezieht sich in der Regel auf die Themen Geldentschädigung sowie die finanzielle Hilfe von verschiedenen Organisationen und Partnern (UN, EU, Rotkreuzgesellschaften und andere). Personen, die solche Anzeigen sehen, sollten keine personenbezogenen Informationen angeben, da es schon zur missbräuchlichen Verwendung von Kreditkartendaten gekommen ist.
    - Über die Website CERT-UA MISP können Organisationen mit dem CERT-UA Informationen über aktuelle Angriffsvektoren und Schwachstellen teilen.
  - **Deutschland:**
    - Information des Landeskriminalamt Baden-Württemberg: „Bisher verzeichnen die Sicherheitsbehörden lediglich Cyberangriffe auf einzelne deutsche Ziele. Zu den befürchteten großflächigen, staatlich gesteuerten Angriffen auf deutsche Ziele kam es bislang glücklicherweise nicht. Dennoch besteht weiterhin ein sehr hohes Risiko für Cyberattacken […].“

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

  - Information des Bundesamts für Sicherheit in der Informationstechnik (BSI): „Nach wie vor stellt das BSI eine erhöhte Bedrohungslage für Deutschland fest. Dies gilt grundsätzlich auch für Kritische Infrastrukturen. Seit Beginn des Angriffs Russlands auf die Ukraine ist es in Deutschland zu einzelnen zusätzlichen IT-Sicherheitsvorfällen gekommen, die aber nur vereinzelt Auswirkungen hatten. […] Das BSI geht insbesondere davon aus, dass grundsätzlich alle Anlagen der Kritischen Infrastruktur – demnach Anlagen zur Versorgung der Allgemeinheit – potenzielles Ziel von Angriffen sein können."

- **Einsatz russischer Antivirensoftware:** Das 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.
- **Desinformationen:** Das Bundesministerium des Innern und für Heimat verzeichnet zuletzt einen signifikanten Anstieg an Medienwebseiten mit prorussischen Desinformationen rund um den Russland-Ukraine-Krieg. So werden nach Aussagen eines Ministeriumssprechers „über Fake-Accounts in bestimmten sozialen Medien täuschend echt aussehende, allerdings gefälschte Webauftritte von etablierten Nachrichtenseiten verlinkt werden."
- **Schadsoftware:** Das U.S. Cyber Command hat gemeinsam mit ukrainischen Sicherheitsbehörden einen Bericht zu Indicators of Compromise, die im Zusammenhang mit in der Ukraine eingesetzter Malware stehen, veröffentlicht.

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 weiterhin die Gefahr, dass russische Cyberkriminelle zur weiteren Destabilisierung der Lage in der Ukraine noch weitreichendere Cyberangriffe als in den letzten Wochen durchführen.

Für die deutsche Industrie

- BSI-Einschätzung: Das BSI sieht eine „erhöhte Bedrohungslage für Deutschland". Daher ruft das BSI „weiterhin Unternehmen, Organisationen und Behörden dazu auf, ihre IT-Sicherheitsmaßnahmen zu überprüfen und der gegebenen Bedrohungslage anzupassen".
- Deutsche Unternehmen sollten weiterhin 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

- Es wird weiterhin allen in der Ukraine tätigen Unternehmen sowie dort lebenden Privatpersonen empfohlen, Updates und Patches immer möglichst schnell zu installieren, um die Cyberresilienz der eigenen Organisation konstant zu wahren.
- 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.
- Seit Ende April 2022 beobachtet das BSI wiederholt Distributed Denial of Service (DDoS)-Angriffe von Hacktivisten auf Ziele in Deutschland und international. Diese Angriffe konnten in den meisten Fällen abgewehrt werden oder hatten nur geringfügige Auswirkungen. Dennoch sollten Unternehmen und Organisationen ein besonderes Augenmerk auf den Schutz gegen diese Art von Angriffen legen. Das BSI hat eine Übersicht zertifizierter DDoS-Mitigations-Dienstleister veröffentlicht.

Mittelfristig

- Im Rahmen des Gesetzes zur Änderung des Energiesicherungsgesetzes 1975 und anderer energiewirtschaftlicher Vorschriften (EnSiGuaÄndG) wird in Artikel 2 Paragraph 2 die Bundesnetzagentur (BNetzA) aufgefordert, bis zum 22. Mai 2023 einen Katalog von Sicherheitsanforderungen für das Betreiben von Energieversorgungsnetzen und Energieanlagen zu erstellen. Dieser solle Kritische Komponenten und kritische Funktionen nach § 2 Abs. 13 Satz 1 Nummer a und b BSIG definieren. Betreiber von Energieversorgungsnetzen und Energieanlagen, die durch Rechtsverordnung gemäß § 10 Absatz 1 Satz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, werden ab sechs Monate nach Veröffentlichung des Kataloges nur noch solche Kritische Komponenten einsetzen dürfen, die nach § 9 Abs. 4 und Abs. 4a in Verbindung mit § 9b zertifiziert und geprüft sind. Hersteller, Inverkehrbringer, Integratoren sowie Betreiber der betroffenen Branchen sollten sich am Konsultationsprozess der BNetzA beteiligen, sobald dieser initiiert wird.