Bundesamt
für Sicherheit in der
Informationstechnik

Nationales IT-Krisenreaktionszentrum BSI

SONDERLAGEBERICHT

Aktuelle Entwicklungen zur Ukraine-Krise

KRZ-Nr. 2022-206425-1133, Version 1.1, 22.03.2022

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:GREEN: Organisationsübergreifende Weitergabe

Informationen dieser Stufe dürfen innerhalb der Organisation und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Redaktioneller Hinweis:
Das Nationale IT-Krisenreaktionszentrum im BSI stellt seinen Zielgruppen **zum Wochenbeginn einen bereinigten Bericht** aus den detaillierten Sonderlagen vom 24.02. bis 18.03.2022 zur Verfügung.

Seit dem frühen Morgen des 24. Februar 2022 führt Russland einen völkerrechtswidrigen Angriffskrieg gegen die Ukraine. Die militärischen Operationen werden weiterhin durch Maßnahmen im Cyberraum begleitet.

Im Wesentlichen ist es in Deutschland zu wenigen unzusammenhängenden IT-Sicherheitsvorfällen gekommen, die aber nur vereinzelt Auswirkungen hatten. Weiterhin positionieren sich verschiedenste Hacker- und Hacktivisten-Gruppierungen im Rahmen der Auseinandersetzung und greifen durch verschiedene Angriffs-Szenarien in den Konflikt ein.
Über das Wochenende 19./20.03.2022 haben sich keine relevanten Sachstandsveränderungen ergeben.
Der Twitteraccount der russischen Botschaft in Großbritannien, mit über 150.000 Followern, soll Medienberichten zufolge, mit anderen Accounts von russischen Botschaften für die Verbreitung von russischer Falschinformationen benutzt werden. Da Regierungsaccounts wie Botschaften bei Twitter eine Sonderrolle in Bezug auf die Compliance-Regeln einnehmen, soll die russische Regierung solche Accounts gezielt für die Verbreitung von Falschinformationen nutzen.
Laut den Berichten hat Twitter bisher nur in Einzelfällen reagiert [NET2022].

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Mehrere ukrainische Nachrichtenwebseiten sollen simultan gehackt und Besuchern das "Z"-Symbol angezeigt worden sein, das als Zeichen der Unterstützung für die russischen Militäroperationen gilt. Das hat der Staatliche Dienst für Sonderkommunikation und Informationsschutz der Ukraine bestätigt. Sie soll über kompromittierte Werbe-Dienste der Webseiten erfolgt sein. Die Manipulation der Webseiten soll inzwischen behoben sein. Die genannte Behörde beschuldigt einen vom russischen Staat unterstützten Akteur [INF2022].
Dem BSI liegen zu diesem Sachverhalt keine belastbaren Erkenntnisse vor.

Sicherheitsforscher der Google Threat Analysis Group (TAG) geben an, staatliche chinesische Akteure bei Cyber-Aktivitäten identifiziert zu haben, die auf ukrainische Regierungsorganisationen abzielten. Die Sicherheitsforscher benachrichtigten die Betroffenen und teilten die IOCs mit Partnern. Google hat angekündigt weitere Informationen zu diesem Sachverhalt zu veröffentlichen [BLE2022].

Aus britischen Regierungskreisen wurde am 18.03.2022 bekannt, dass zwei Minister*innen gefälschte Anrufe erhalten haben, in denen sich die Anrufer als der ukrainische Premierminister Denys Shmyhal ausgaben. Es soll sich um zehnminütige, aufwändiger inszenierte Videokonferenzen gehandelt haben. Es gibt derzeit keinen Hinweis darauf, dass "Deepfake"-Technologie zum Einsatz kam. Laut der britischen Regierung soll es sich um "desinformation on behalf of the Kremlin" handeln. Die Nachrichtenagentur gibt an, dass die Anrufer versuchten, Informationen über die britische Politik bzgl. der Ukraine zu erhalten [BBC2022].

Update 22.03.2022:
Die russische Sberbank, warnt ihre Kunden vor Softwareaktualisierung von Software. Auslöser für die Warnung ist sogenannte "Protestware". Dabei wird von den Softwareentwicklern aus Protest gegen den Einmarsch Russlands in die Ukraine bösartiger Code in Open-Source-Software eingeschleust. Ausgeführt wird der Schadcode, wenn das System eine IP-Adresse aus Russland oder Belarus bezieht [TVE2022]. Dieser Sachverhalt ist im Zusammenhang mit unserer Meldung vom 18.03.2022 zu sehen. Dort berichteten wir bereits über den Supply-Chain-Angriff durch das npm-Paket "node-ipc".
Aus den Meldungen zur Warnung der Sberbank geht nicht eindeutig hervor, ob sich die Sberbank auf allgemeine Software bezieht oder ob in der Betrachtung eigene Bankingsoftware im Fokus steht.

Am 14.03.2022 berichteten wir über die Bestrebung der russischen Generalstaatsanwaltschaft, den facebook-Mutterkonzern "Meta" als extremistische Organisation einzustufen und verbieten zu lassen. Dazu wurde am 21.03.2022 bekannt, dass die beiden Dienste "facebook" und "Instagram" durch ein russisches Gericht verboten wurde. Das Gericht begründet sein Urteil damit, dass der Mutterkonzern Aufrufe zur Gewalt gegen russische Soldaten auf seinen Plattformen zulasse [TAG2022].

Das Hackerkollektiv Anonymous hat über den Kurznachrichtendienst Twitter internationale Unternehmen dazu aufgefordert, sich kurzfristig aus Russland zurückzuziehen. Dabei zielt die Kampagne nach derzeitigem Sachstand auf Unternehmen ab, die in Russland Steuern für ihre geschäftliche Tätigkeit abführen und damit "den Militärapparat Russlands unterstützen". Anonymous nennt in seinen Botschaften verschiedene bekannte Unternehmen wie bspw. Metro AG, Citrix, Nestlé oder auch österreichische Raiffeisen Banken [TWI2022].

Bewertung

Die **erhöhte Bedrohungslage** für Deutschland im Zusammenhang mit der Ukraine-Krise bleibt **unverändert** bestehen. Diese Situation kann sich nach Einschätzung des BSI jederzeit ändern.

Der Konflikt wird weiterhin von verschiedensten Formen von Cyber-Angriffen begleitet.
In Bezug auf die gefälschten Videokonferenzen mit hochrangigen Mitgliedern der britischen Regierung rät das BSI zur erhöhten Vorsicht im Zusammenhang mit möglicher Kontaktanbahnung sowie weiterhin mit den verschiedensten Formen der Desinformation. Auch deutsche Institutionen der Politik, dem politiknahen Umfeld sowie der Wirtschaft könnten Ziel derartiger Kampagnen werden.

Update 22.03.2022:
Die **erhöhte Bedrohungslage** für Deutschland im Zusammenhang mit der Ukraine-Krise bleibt **unverändert** bestehen. Diese Situation kann sich nach Einschätzung des BSI jederzeit ändern.

Der Konflikt wird weiterhin von verschiedensten Formen von Cyber-Angriffen begleitet.

Die Botschaft des Hackerkollektivs Anonymous zeigt, dass mit weiteren Cyber-Angriffen gegen "westliche" KRITIS-Unternehmen und daraus resultierenden KRITIS-Schäden in "westlichen" Staaten zu rechnen ist.

Maßnahmen

Die Maßnahmenempfehlungen des BSI aus den vorangegangenen Berichten bleiben bestehen. Das BSI rät weiterhin zur erhöhten Wachsamkeit.
Zum Themenkomplex "Hoax (Falschmeldungen)" stellt das BSI weiterführende Informationen auf seiner Webseite bereit [BSI2022].

Update 22.03.2022:
Im Zusammenhang mit der Botschaft, sowie dem durch Teile des Hackerkollektivs erfolgten Cyber-Angriff auf einen Betreiber der deutschen KRITIS-Branche Mineralöl, weist das BSI nochmals auf seine bisherigen Maßnahmenempfehlungen sowie die Sicherung von Fernwartungszugängen (OPS.1.2.5 Fernwartung) hin [BSI2022a] und rät zur dringenden Umsetzung.
Das BSI rät weiterhin zur erhöhten Wachsamkeit.

Links

[NET2022] https://netzpolitik.org/2022/falschinformationen-wie-russland-die-desinformationsregeln-von-twitter-umgeht/
[INF2022] https://www.infosecurity-magazine.com/news/russian-hackers-ukrainian-news-z/
[BLE2022] https://www.bleepingcomputer.com/news/security/google-chinese-state-hackers-target-ukraine-s-government/
[BBC2022] https://www.bbc.com/news/uk-politics-60824956
[BSI2022] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Hoax-Falschmeldung/hoax-falschmeldung.html
[TVE2022] https://www.theverge.com/2022/3/21/22989339/protestware-attacks-russia-sberbank-open-source
[TAG2022] https://www.tagesschau.de/ausland/europa/russland-meta-facebook-instagram-verbot-101.html
[TWI2022] https://mobile.twitter.com/YourAnonTV/status/1505679705797713927
[BSI2022a] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.