Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

# Sonderlagebericht des Nationalen IT-Krisenreaktionszentrums

*Aktuelle Entwicklungen zur Ukraine-Krise*

*CSW-Nr. 2022-197345-1032, Version 1.0, 24.02.2022*

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:WHITE: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben 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

Am frühen Morgen des 24. Februar 2022 kam es zu einer Invasion russischer Kräfte in das Staatsgebiet der Ukraine. Diese militärische Operation wurden durch Verfügbarkeitsangriffe auf Webseiten sowie Sabotage-Angriffe (Wiper) auf ausgewählte ukrainische Institutionen begleitet:

- Die DNS-Amplification DDoS-Angriffe waren auf Webseiten zweier ukrainischer Banken und auf Webseiten ukrainischer Ministerien sowie des Parlaments beschränkt.
- Nahezu zeitgleich wurden Daten-Lösch-Programme, sogenannte Wiper, auf ukrainischen Rechnern entdeckt.
  Betroffen waren (ungenannte) Banken, sowie Dienstleister der ukrainischen Regierung mit Sitz in Litauen und Lettland. Der genaue Zweck der Wiper-Angriffe ist bisher nicht bekannt.
  Der Wiper besitzt keine neuen Methoden für den Angriffsvektor und keine automatisierte Verbreitungsfunktion. In Teilen scheint er auf im Vorfeld infizierte Systemen zum Einsatz gekommen zu sein.
  Da die Schadprogramme in einigen Fällen über Windows Group Policies verteilt wurden, müssen die Täter bereits entsprechende Administrator-Rechte und Zugang zu zentralen Servern gehabt haben.

Mehrere NATO-Partner sehen seit dem heutigen Tag vermehrte aggressive Scan-Aktivitäten in ihren Netzen.

* 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.



BSI IT-Sicherheitsinformation

Für die Bundesrepublik Deutschland wurden dem Nationale IT-Krisenreaktionszentrum im Bundesamt für Sicherheit in der Informationstechnik **keine Auffälligkeiten gemeldet bzw. durch dieses festgestellt**.

Das BSI hat in jüngster Vergangenheit bereits vor möglichen Kollateralschäden durch Angriffe auf ukrainische Unternehmen gewarnt. Die Warnungen wurden an verschiedene Zielgruppen des BSI verteilt und enthielten im Wesentlichen die unten aufgeführten Maßnahmenempfehlungen.

# Bewertung

Das Nationale IT-Krisenreaktionszentrum sieht **aktuell keine geänderte Gefährdung für deutsche Stellen** und rät zur erhöhten Wachsamkeit, Reaktionsbereitschaft und zur Umsetzung der im Folgenden beschriebenen Maßnahmenempfehlungen.

# Maßnahmen

Das Nationale IT-Krisenreaktionszentrum empfiehlt weiterhin die Umsetzung folgender Maßnahmen (aus den Warnmeldungen):

## Übergreifende und infrastrukturelle Maßnahmen

- **Erreichbarkeiten / Verfügbarkeit**
  Die Verfügbarkeit (ggf. Urlaubssperre, Freigabe von Überstunden-Aufbau und Mehrarbeit zu ungünstigen Zeiten, interne Verlagerung von Personal etc.) und Erreichbarkeit des notwendigen Personals (eigenes Personal, sowie auch Personal von Dienstleistern) für die Präventions- und Reaktionsmaßnahmen sollte konkret für die nächsten Wochen geprüft und sichergestellt werden. Deren Erreichbarkeiten sollten auch offline dokumentiert verfügbar sein.
- **BCM-Notfallpläne prüfen, dabei auch Schadensbewältigung ohne externe Dienstleister berücksichtigen**
  Bei großflächigen Auswirkungen von Cyber-Angriffen werden eine Vielzahl an Unternehmen gleichzeitig externe Unterstützung durch Dienstleister benötigen. Aufgrund der begrenzten Kapazitäten dieser, werden aber nicht alle Unternehmen konkret unterstützt werden können.Sie sollten daher in den BCM-Notfallplänen auch eine Schadensbewältigung ohne die Unterstützung externer Dienstleister als Rückfalloption berücksichtigen.Das BSI bereitet sich darauf vor, in so einem Fall (vgl. Exchange-Schwachstellen 2021) skalierende zentrale Unterstützungsmaßnahmen (z.B. CSW, Hilfedokumente, Webinare, Telkos, ...) bereit zu stellen.

## Angriffsfläche minimieren

- **Systeme auf aktuellen Patchstand bringen und Einspielen von Notfallpatches vorbereiten**
  Wenn Hersteller bei 0-Day Schwachstellen Patches veröffentlichen, sollten diese auch kurzfristig (24/7) installiert werden.Dazu sollten mindestens bei allen externen Systemen kurzfristig die verfügbaren Sicherheitspatches installiert werden, siehe mindestens Top-Schwachstellen [CISA2022]. Auch wenn die Empfehlung der Installation aller ausstehenden Sicherheitspatches sehr unspezifisch ist, ist der Aufwand hierfür sehr gering. Daher hat diese Maßnahme ein sehr hohes Nutzen/Aufwand-Verhältnis und minimiert die eigene Angriffsfläche erheblich.
- **Härtung aller Systeme mit Zugriffsmöglichkeit von außen**
  Unternehmen verfügen in der Regel über eine Mehrzahl von Systemen mit Außenanbindung, z. B. VPN, RDP, OWA, Exchange-Online, Extranet-Portale, uvam. Bei Ransomware-Angriffen wurden bereits in der Vergangenheit gezielt Mitarbeitende von Unternehmen auch privat angegriffen, um dann über deren sowohl privat als auch beruflich genutzte Passwörter ins Unternehmensnetz einzudringen. Daher sollten alle Logins mit Außenanbindung über eine Multi-Faktor-Authentifizierung (MFA) geschützt werden. Falls eine MFA zeitnah nicht aktivierbar ist, sollten mindestens kurzfristig neue, komplexe, für jedes System unterschiedliche Passwörter verwendet werden, siehe [BSI2019a] und [BSI2020a]. Dies gilt vor allem für Admin-Konten. Sofern dies nicht technisch zu erzwingen ist, sollte dies durch organisatorische Maßnahmen, z. B. gegen Unterschrift bestätigt, umgesetzt werden.

- **Härtung von Admin-Systemen**
  Admin-Systeme dürfen nur für administrative Aufgaben und nicht für das "Tagesgeschäft" (z.B. persönliche E-Mails, Internet-Recherche, ...) genutzt werden. Dabei sollten bei unterschiedlichen Netzen auch unterschiedliche Admin-Konten sowie Admin-Systeme mit unterschiedlichen Credentials verwendet werden.
- **Erschwerung von Lateral Movement ins/innerhalb des internen Netzwerks**
  Eine Kompromittierung externer Systeme und Netze, z. B. einer DMZ, darf nicht zur Kompromittierung wichtiger interner Systeme führen. Es gilt, die Vertrauensbeziehungen zwischen diesen Systemen zu minimieren und verschiedene Accounts mit verschiedenen Passwörtern in den jeweiligen Netzen zu nutzen.

### Detektion verstärken, um Angriffe schnellstmöglich zu entdecken

- **IT-Sicherheits-Logging und -Monitoring**
  Insbesondere Zugriffe auf externe Systeme sollten intensiviert mit geeigneten Lösungen und geschultem Personal überwacht werden.

### Reaktionsmaßnahmen vordenken, vorbereiten und lageangepasst umsetzen

- **Backups erstellen und prüfen**
  Aktuelle sichere Backups sollten von allen relevanten Systemen existieren. Eine Kopie der Backups sollte offline gelagert werden.
- **Recovery vorbereiten und testen**
  Die Wiederherstellung von Systemen, insbesondere von relevanten Systemen (File-, Mail-, AD-Server, DB, krit. Fachverfahren...) sollte getestet werden. Erfahrungsgemäß kommt es bei einer erstmaligen Wiederherstellung oder einer ersten Wiederherstellung nach längerer Zeit oftmals zu unvorhergesehenen Problemen, die ein Recovery erschweren oder sogar verhindern, insb. bei Fachverfahren und Datenbanken.Dazu sollten Pläne für eine Wiederherstellung nach totalem Datenverlust ("Schwarz-Start") existieren, bei dem alle Systeme aus den Backups wiederhergestellt werden müssen, z.B. nach Verschlüsselung auf Virtualisierungs-Server-Ebene.

### Aufwuchs- und Durchhaltefähigkeit planen

- **Erhöhung der Funktionsfähigkeit von IT-Betrieb, SOC und CERT bei Lageverschärfung**
  Sollte es zu einer Verschärfung der Bedrohungslage kommen, sollten Sie sicherstellen, dass der IT-Betrieb, sowie das Unternehmens Security Operations Centre (SOC) und/oder Computer Emergency Response Team (CERT) in eine erhöhte Funktionsbereitschaft wechseln. Angefangen bei einer 24/7 Rufbereitschaft, über 24/7 Schichtdienst bis hin zu einer besonderen Aufbauorganisation (BAO) im Rahmen des Unternehmens-Krisenmanagements. Die BAO sollte von Anfang an durchhaltefähig geplant werden.

Die Auflistung der Maßnahmen ist nicht abschließend und muss eigenständig im Rahmen der Vorbereitung individuell an die eigenen Rahmenbedingungen angepasst und erweitert werden.

## Links

# 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.