Bundesamt
für Sicherheit in der
Informationstechnik

TLP:WHITE

Deutschland
Digital•Sicher•BSI•

Maßnahmenempfehlungen des BSI im Hinblick auf die aktuelle Lage in der Ukraine

28.02.2021

Folgende Maßnahmen sollten geprüft und ggf. kurzfristig umgesetzt bzw. verbessert werden

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

Maßnahmenempfehlungen des BSI

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.

Maßnahmenempfehlungen des BSI

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. 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. 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.

Maßnahmenempfehlungen des BSI

Angriffsfläche minimieren

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.

Maßnahmenempfehlungen des BSI

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.

Maßnahmenempfehlungen des BSI

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.

TLP:WHITE

Deutschland
Digital•Sicher•BSI•

Kontakt

CERT-Bund, Referat OC21 - Grundsatz und Warn- und Informationsdienst WID
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 -189
53175 Bonn
Telefon: +49 228 99 9582-5110
E-Mail: lagezentrum@bsi.bund.de

Internet: www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik