Alarmstufe Rot

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY

Es liegt eine besondere Bedrohungslage vor Informationssicherheitskrise

Die deutschen Behörden sowie die IT-Sicherheitsbehörde BSI warnen Firmen vor russischen Hackerangriffen, insbesondere Firmen der kritischen Infrastrukturen. Viele relevante Stellen sind bereits in Hinblick auf deren IT-Infrastruktur sensibilisiert.

Der Verfassungsschutz sowie die IT-Sicherheitsbehörde BSI rechnen mit Sabotageattacken in der Ukraine. Wegen möglicher Kollateralschäden in der Bundesrepublik sollten Firmen sensibilisiert sein und mit Cyberexperten in Kontakt stehen.

Wegen der Vernetzung vieler Systeme seien Kollateralschäden in Deutschland nicht ausgeschlossen. Betroffen sein könnten Politik, Verwaltung und für die Infrastruktur Deutschlands wichtige Unternehmen. Dazu zählt etwa der Energiesektor.

So sollten z.B. Sicherungskopien von allen relevanten Systemen angelegt werden. Ferner sind weiterführende Maßnahmen nach Ansicht des BSI ohnehin notwendig.

Destruktive Malware wurde die in den Stunden vor der Invasion gegen Ziele in der Ukraine und anderen Ländern der Region eingesetzt.

Die Ukraine wurde seit Beginn des Konflikts mit Russland bereits mehrfach mit Cyberangriffen konfrontiert, so z.B. am Mittwoch, den 23.02.2022, als die Website des ukrainischen Parlaments sowie mehrere Banken und Regierungsstellen angegriffen wurden.
Kurz vor dem Beginn der russischen Invasion, am Morgen des 24. Februar, wurde eine neue Form von Malware (Trojan.Killdisk) zum Löschen von Festplatten eingesetzt, um Organisationen in der Ukraine anzugreifen.

Schon im Januar waren mehrere Internetseiten der ukrainischen Regierung massiv attackiert worden. Vorübergehend konnten die Webseiten der Außen-, Katastrophen- und Forschungsministerien nicht aufgerufen werden.

Die gezielten Cyberangriffe auf die Ukraine könnten Auswirkungen über die Grenzen des Landes hinaus haben (sowohl physisch als auch virtuell), so z.B. auf Unternehmen, Regierungen und andere Parteien in der Region. Da die Invasion nun im Gange ist, ist die Wahrscheinlichkeit weiterer Cyberangriffe auf die Ukraine und andere Länder in der Region weiterhin hoch.

Unternehmen weltweit, die mit Organisationen in der Ukraine zusammenarbeiten, müssen besonders vorsichtig sein, fügten die Analysten hinzu, "da Verbindungen zu ukrainischen Systemen als Dreh- und Angelpunkt für andere Ziele genutzt werden könnten".
Digitale Angriffe flankieren heutzutage moderne Kriege und sind Teil einer hybriden Kriegsführung.

Be Aware und informieren Sie Ihr Cyber Rapid Response Team.

Verwandte Bedrohungsgruppen und Wirkungen

Unsere Cyber Threat Intelligence Experts bewertet die folgenden Gruppen:

SANDFISH: Angriffe durchgeführt auf politische Einrichtungen, Presse und kritische Infrastrukturen.
WINTERFLOUNDER: Angriffe auf der die ukrainischen Regierung, Militär und die Strafverfolgungsbehörden.
WALLEYE: Gegen staatliche Institutionen, Sicherheitsorgane und die Militärindustrie in Osteuropa, dem Nahen Osten sowie Süd- und Zentralasien.

Maßnahmen zum Aufbau und Stärkung Ihrer Cyber-Resilienz

In diesem Zusammenhang empfehlen wir Ihnen, Cybersicherheitsmaßnahmen umzusetzen und Ihre Überwachung zu verstärken. Wir weisen Sie darauf hin, sicherzustellen, dass Sie die wichtigsten IT-Hygienemaßnahmen richtig umsetzen, alle empfohlenen Best Practices berücksichtigen und die Warnungen und Sicherheitshinweise auch des BSI aufmerksam verfolgen.
Um die Risiken von Cyber-Bedrohungen zu begrenzen, schlägt unser Expertenteam die folgenden strategischen und operationellen Sofortmaßnahmen vor, die Sie im Falle einer Krise ergreifen können.

- Erstellung eines angemessenen Vorfallsreaktionsplans (IR) und Aufbau eines Ausfallsicherheitsplans
- Verstärkung der Authentifizierung auf Ihre Informationssystemen
- Sicherstellung, eines geeignetes Krisenmanagement für alle mögliche Cyberangriffe
- Erstellung einer priorisierten Liste der kritischen digitalen Dienste Ihrer Organisation
- Definition von Notfallkontaktstellen, auch bei digitalen Dienstleistern, und die Sicherstellung, dass die Nummern in Papierform vorliegen, ist in solchen Situationen besonders hilfreich
- Erstellung eines Reaktionsplans auf Cyberangriffe, um die Kontinuität der Geschäftsabläufe und deren Rückkehr in einen nominalen Zustand zu sichern
- Umsetzung eines IT-Kontinuitätsplan
- Definition eines IT-Wiederherstellungsplan
- Erhöhung der Sicherheitsaufsicht
- Behandlung von Malware-Erkennungen
- Tests Durchführung von Backup-Verfahren
- Überwachung der Domänencontrollern
- Überwachung von Dienstkonten und Administratorkonten
- Überwachung der Installation von Dateiübertragungs-Tools und Programmen
- Erstellung, Pflege und regelmäßige Überprüfung der Cybervorfälle und die Kontinuität des Betriebs
- Implementierung einer Netzsegmentierung zwischen IT- und OT-Netzen
- Umsetzung wirksamer Richtlinien für Anmeldedaten und Passwörter, Ablehnung schwacher Passwörter oder Durchsetzung von Regeln für sichere Passwörter
- Einführung starker Verschlüsselungsverfahren, um zu verhindern, dass Bedrohungsakteure auf sensible Daten zugreifen können
- Implementierung von Systemen zur Erkennung von E-Mail-Anomalien, um Spear-Phishing-Links zu erkennen
- Offline-Sicherung der kritischer Daten

Alarmstufe Rot

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY

BE AWARE !

Für eine hohe Bereitschaft zur Krisenbewältigung im Cyberspace, wird die Anwendung der hier aufgeführten Maßnahmen dringend empfohlen.
Wir empfehlen unseren Partnern und Kunden, verstärkt auf Cyber Threat Intelligence zu setzen, um versteckte Anomalien in Datensätzen aufzuspüren. Unsere Experten beraten zu IT-effizienten Methoden, mit denen Anomalien in Echtzeit-Datenströmen automatisch erkannt werden können.

We Keep Threats at Bay!
samapartners.com