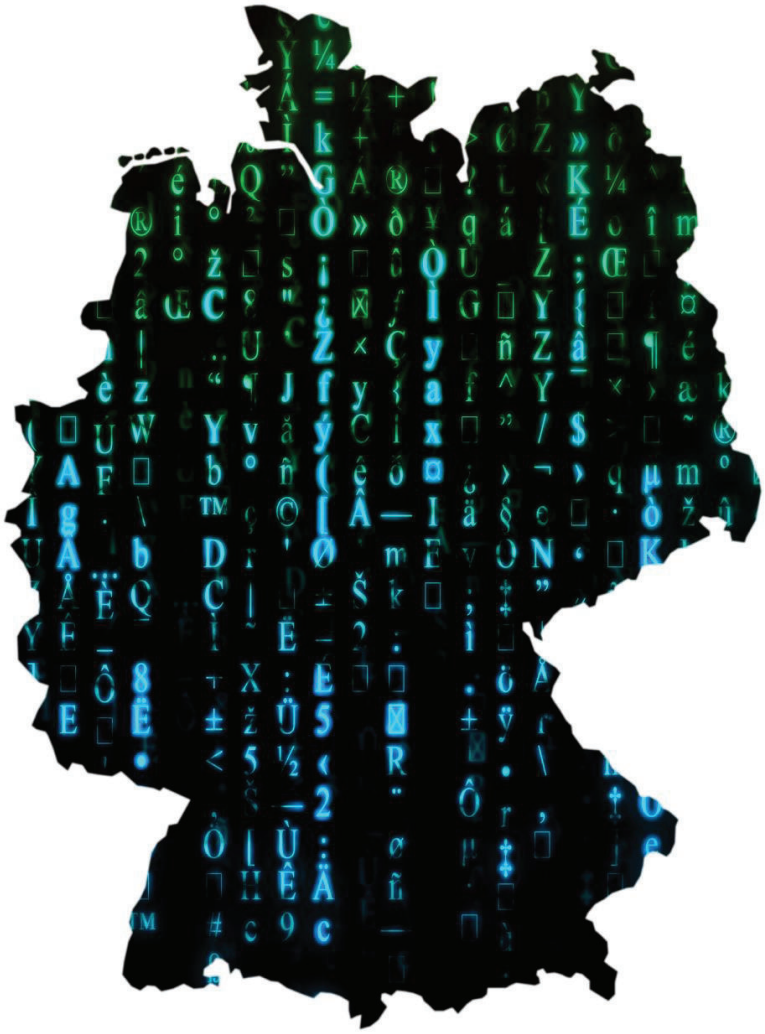
~~VS – NUR FÜR DEN DIENSTGEBRAUCH~~

Nationales Cyber-Abwehrzentrum

Cyber-Lage

- 22. Dezember 2015 -



Themen

Meldezeitraum

Montag, 21.12.2015, 09:00 Uhr - Dienstag, 22.12.2015, 09:00 Uhr

Verteiler

Cyber-AZ-Behörden:	BAAINBw, BBK, BfV, BITS, BKA, BND, BPOL, BSI, MAD, ZKA
Fachaufsichten, Cyber-Sicherheitsrat:	AA, BKAmt, BMBF, BMF, BMI, BMJV, BMWi, BMVg, HMDIS Hessen, IM BW

Weiterverteilung

Die Weiterverteilung der „Cyber-Lage“ an die Verfassungsschutzstellen der Länder erfolgt über das BfV, die Verteilung an die LKÄ über das BKA und die Verteilung an die regionalen MAD-Stellen über den MAD.

Eine Weitergabe an hier nicht aufgeführte Stellen bedarf der Zustimmung des Cyber-AZ.

Inhaltliche Ausrichtung

Die „Cyber-Lage“ des Nationalen Cyber-Abwehrzentrums wird arbeitstäglich erstellt und enthält Sachverhalte mit Bezug zum Thema Cyber-Sicherheit, die eine hohe technische, politische und/oder mediale Relevanz aufweisen.

Herausgeber

Nationales Cyber-Abwehrzentrum
c/o Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

E-Mail: cyber-az@bsi.bund.de
Tel.: 0228 99 9582 6000

USA: FBI ermittelt nach Fund von Schadcode in Netzwerkfirmware

Sachverhalt

Ende voriger Woche teilte das US-amerikanische Unternehmen *Juniper Networks* mit, im Rahmen routinemäßiger Untersuchungen sei nicht autorisierter Programmcode in dem hauseigenen Produkt *ScreenOS* erkannt worden.[1]

Juniper Networks gehört zu den weltweit größten Herstellern von Netzwerkkomponenten. Zu seinen Kunden zählen u. a. namhafte Unternehmen der Branche Telekommunikation. *ScreenOS* ist ein Betriebssystem, das als Firmware in den hauseigenen Netzwerkprodukten eingesetzt wird.

Der gefundene illegale Code stellt eine sog. Backdoor dar. Er erlaubt die missbräuchliche Ausführung beliebiger Kommandos mit Administratorrechten. Dadurch ist es möglich, die vollständige Kontrolle über das betroffene Gerät zu übernehmen. Inzwischen hat *Juniper Networks* einen Patch veröffentlicht, der diese Sicherheitslücke schließen soll. Deren Ausnutzung sei laut Presseberichten (z. B. *Heise Online*[2]) über einen Zeitraum von rund drei Jahren möglich gewesen.

Das US-amerikanische FBI hat Ermittlungen zu dem Sachverhalt aufgenommen. Grund dafür könnte sein, dass große US-Unternehmen und Regierungsdienststellen zu den Kunden von *Juniper Networks* gehören.

Davon unberührt befindet sich laut Hersteller eine weitere, bislang nicht geschlossene Schwachstelle in einer Kryptografie-Komponente von *ScreenOS*. Durch Ausnutzung dieser Schwachstelle könnte der Netzwerkverkehr über eine vermeintlich sichere VPN-Tunnelverbindung mitgelesen werden.[3] Die Berichte zu dieser zweiten Schwachstelle werden vielfach von Hypothesen zu einer staatlich gesteuerten Urheberschaft begleitet.

Derzeit sind weltweit rund 27.000 Geräte im Internet erreichbar, die potenziell von den Schwachstellen betroffen sind. Davon befinden sich ca. 900 in Deutschland.[4]

Bewertung

Das *CERT-Bund* stuft den Sachverhalt als äußerst kritisch ein.

Gründe für diese Bewertung

- Das für die missbräuchliche Aneignung von Administratorrechten benötigte Kennwort wird bereits über einschlägige Kanäle verbreitet
- Die potenzielle Schadwirkung (z. B. Ausspähung von VPN-Verbindungen) ist erheblich
- Der schädigende Code ist aus der Distanz ausführbar

Maßnahmen

Das *CERT-Bund* hat eine technische Sicherheitswarnung erstellt und an folgende Informationskreise verteilt:[5]

[1] https://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554

[2] http://www.heise.de/newsticker/meldung/Schnueffelcode-in-Juniper-Netzgeraeten-Weitere-Erkenntnisse-und-Spekulationen-3051260.html

[3] http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST

[4] http://www.pentest.guru/index.php/2015/12/21/juniper-screenos-backdoor-attack-demystified/

[5] BSI-IT-Sicherheitswarnung Nr. 2015-226773-1000, Version 1.0, 21.12.2015: „Kritische Schwachstellen von Juniper ScreenOS ermöglichen komplette Systemkompromittierung“

- UP Bund
- VerwaltungsCERT-Verbund
- UP KRITIS
- Allianz für Cyber-Sicherheit

Handlungsempfehlungen

Die IT-Sicherheitsverantwortlichen der genannten Informationskreise haben die technischen Empfehlungen des BSI bereits mit o. g. Sicherheitswarnung erhalten.

Für die Adressaten der Cyber-Lage ergeben sich keine besonderen Empfehlungen.