Betreff: AW: Anfrage Deauthentication/Rogue AP Containment
Von: "Service-Center BSI" <service-center@bsi.bund.de>
Datum: 17.10.2019, 15:25
An: "'Marcel Langner'" [redacted]
Return-Path: <service-center@bsi.bund.de>
Received: [redacted] by mail.localdomain with POP3 (fetchmail-[redacted]) for [redacted] (single-drop); Thu, 17 Oct 2019 15:25:01 +0200 (CEST)
Received: from mailgwbsi.officedirekt-servicecenter.de (mailgwbsi.officedirekt-servicecenter.de [93.190.68.25]) [redacted] with ESMTPS id x9HDOeBL007577 (version=TLSv1.3 cipher=TLS_AES_256_GCM_SHA384 bits=256 verify=NOT) for [redacted] Thu, 17 Oct 2019 15:24:42 +0200
Received: from ofwaec104 (unknown [217.6.125.154]) (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (No client certificate requested) (Authenticated sender: service-center@bsi.bund.de) by mailgwbsi.officedirekt-servicecenter.de (Postfix) with ESMTPSA id 32DF21F3CA; Thu, 17 Oct 2019 15:24:40 +0200 (CEST)
[redacted]
Nachricht-ID: <007201d584ee$56088720$02199560$@bsi.bund.de>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="----=_NextPart_000_0073_01D584FF.1993C820"
X-Mailer: Microsoft Outlook 16.0
Thread-Index: AQHVgHarj6Y2NwFxlEyuv/NdHuKqtade24Sw
Content-Language: de

Sehr geehrter Herr Langner,

vielen Dank noch einmal für Ihre Rückmeldung.

Bitte entschuldigen Sie das Missverständnis und die späte Beantwortung Ihrer E-Mail.

Zu (1) und (2): Containment Funktion

Der Baustein NET.2.1 WLAN-Betrieb regelt unter dem Punkt NET.2.1.A12 den Einsatz einer geeigneten WLAN-Management-Lösung [1]. Hierbei handelt es sich um eine Standard-Anforderung dar. Die dazugehörige Maßnahme unter dem Punkt NET.2.1.M12 [2] empfiehlt eine Rogue Access Point Detection Funktionalität. Darüber hinaus werden 3 fiktive Szenarien beschrieben, die Mindestparameter zur Erkennung von Manipulationen und Angriffen zugeordnet werden.

Es wird u.a. empfohlen, dass der Missbrauch von „gültigen“ SSIDs in Verbindung mit einer unverschlüsselten Kommunikation detektiert wird.

Eine Aussage zu möglichen aktiven Gegenmaßnahmen, wie z. B. die von Ihnen angesprochene Containment Funktion, enthält der Baustein NET.2.1 WLAN-Betrieb nicht.

Bei der Fragestellung, ob die Nutzung einer Containment Funktion zulässig ist, handelt es sich um eine rechtliche Fragestellung. Ich bitte um Ihr Verständnis, dass das BSI grundsätzlich keine Rechtsberatung übernehmen kann. Diese ist gem. Rechtsdienstleistungsgesetz den dort abschließend genannten Berufsgruppen vorbehalten.

Gegebenenfalls kann Ihnen die Bundesnetzagentur zur Zulässigkeit einer solchen Funktion Hinweise geben.

Zu 3): Regelung im Rahmen unserer Zertifizierung

Nein, es gibt keine Regelung im Rahmen der Zertifizierung, die die es erfordert, eine solche Funktion einzusetzen, um die Zertifizierung zu erhalten.

Zu 4): Entzug einer Zertifizierung

Nein, es ist nicht mit dem Entzug einer Zertifizierungen zu rechnen, sofern eine Hochschule solche Funktionen einsetzt (siehe Punkt 3).

Bezüglich Verletzung anderer Gesetze: Auch hierzu können wir Ihnen leider keine Auskunft geben. Die konkrete rechtliche Bewertung eines Einzelfalls stellt eine Rechtsberatung dar (siehe (1) und (2)).

[1]https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_2_1_WLAN-Betrieb.html

[2]https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/NET/Umsetzungshinweise_zum_Baustein_NET_2_1_WLAN-Betrieb.html

Mit freundlichen Grüßen,
Im Auftrag

[redacted]

Bundesamt fuer Sicherheit
in der Informationstechnik

Service-Center

Postfach 20 03 63
53133 Bonn

E-Mail: service-center@bsi.bund.de
Tel.: +49 0800 - 2741000
Fax: +49 0800 - 274600

++++ Sind Sie schon Abonnent unseres Bürger-CERT Newsletters?

Anmeldung unter https://www.bsi-fuer-buerger.de/Buerger-CERT ++++

Von: Marcel Langner [redacted]
Gesendet: Freitag, 11. Oktober 2019 22:49
An: Service-Center BSI <service-center@bsi.bund.de>
Betreff: Re: Anfrage Deauthentication/Rogue AP Containment

Sehr geehrte Damen und Herren,
ich habe bisher keinerlei Rückmeldung zu meiner unten angefügten Nachfrage erhalten.

Am 30.09.2019 um 19:19 schrieb Marcel Langner:

> Sehr geehrte Damen und Herren,
> vielen Dank für Ihre Antwort. Leider erscheint es mir, als hätte ich mich missverständlich ausgedrückt.
> Aus Ihrer Antwort lese ich eine Stellungnahme zur Rogue Accesspoint DETECTION Funktion.
> Meine Frage bezog sich jedoch auf die Rogue Accesspoint CONTAINMENT Funktion. Diese unterscheidet sich von der Detektion dadurch, dass unmittelbar nach Detektion der erkannte Rogue mit Deauthpaketen attackiert wird.
> Einige Hochschule definieren den Rogue dann so, dass dieser noch nicht einmal die gleiche SSID aussenden muss. Es wird also JEDER Accesspoint auf dem Gelände der Hochschule durch die Hochschulsysteme attackiert.
>
> Darf ich höflichst um die Stellungnahme zu diesem Verhalten und meinen ursprünglichen 4 Fragen bitten?
> Entschuldigen Sie bitte meine missverständliche Ausdrucksweise und die Arbeit, die ich Ihnen bereite.
>
> Hochachtungsvoll
> Marcel Langner
>
> Am 30.09.2019 um 15:52 schrieb Service-Center BSI:
>
> > Sehr geehrter Herr Langner,
> >
> > zunächst einmal vielen Dank für Ihre E-Mail und entschuldigen Sie bitte die späte Beantwortung Ihrer E-Mail.
> >
> > A. Hintergrundinformationen (Anforderungen / Umsetzungshinweise) Der IT-Grundschutz unterscheidet zwischen Basis- und Standard-Anforderungen sowie Anforderungen bei erhöhtem Schutzbedarf.
> > Basis-Anforderungen müssen vorrangig umgesetzt- Bei den Basis-Anforderungen handelt es sich um uneingeschränkte Anforderungen bzw. uneingeschränkte Verbote. Sie bilden die Grundlage für die Vorgehensweise "Basisabsicherung".
> >
> > Standard-Anforderungen bauen auf den Basis-Anforderungen auf und adressieren gemeinsam mit diesen den normalen Schutzbedarf. Sie sollten umgesetzt werden, bzw. darin genannte Aspekte sollten nicht erfolgen. Die Umsetzung der hier aufgeführten Anforderungen ist grundsätzlich erforderlich, aber nicht vorrangig. Es können unter bestimmten Umständen Gründe vorliegen, einen bestimmten Aspekt anders, nur teilweise oder gar nicht umzusetzen, die vollständigen Implikationen müssen jedoch klar und sorgfältig abgewogen und dokumentiert werden. Liegen solche Gründe nicht vor, sind Standard-Anforderungen analog zu Basis-Anforderungen als uneingeschränkte Anforderungen bzw. Verbote zu verstehen.
> >
> > Mit den Anforderungen bei erhöhtem Schutzbedarf werden exemplarisch Beispiele erprobter Empfehlungen für den höheren Schutzbedarf gegeben, die als Grundlage für die erforderliche Risikoanalyse dienen können. Sie sollten erfüllt werden, wenn erhöhter Schutzbedarf vorliegt.

Zu vielen Bausteinen des IT-Grundschutz-Kompendiums gibt es detaillierte Umsetzungshinweise. Diese beschreiben konkret, wie die Anforderungen der Bausteine umgesetzt werden können und erläutern im Detail geeignete Sicherheitsmaßnahmen. Die Sicherheitsmaßnahmen können als Grundlage für Sicherheitskonzeptionen verwendet werden, sie sollten aber an die Rahmenbedingungen der jeweiligen Institution angepasst werden. Anders als die Anforderungen aus den Bausteinen sind die Maßnahmen für den Anwender nicht verbindlich, sondern sollen bewährtes Vorgehen und Best Practices aufzeigen, um den Anwender bei der Erfüllung der Anforderungen zu unterstützten.

B. Stellungnahme
Zu 1) und 2)
Aus unserer Sicht können solche Funktionen zur Verbesserung sowohl der Sicherheit des Netzes als auch der Servicequalität (falls Sie mit Servicequalität die Verfügbarkeit meinen) beitragen, wenn sie mit Bedacht verwendet werden. Der Baustein NET.2.1 WLAN-Betrieb regelt unter dem Punkt NET.2.1.A12 den Einsatz einer geeigneten Management-Lösung. In der dazugehörigen Maßnahme NET.2.1.M12 "Einsatz einer geeigneten Magement-Lösung" wird empfohlen, eine Rogue Access Point Detection Funktionalität einzusetzen. Hierbei empfehlen wir dringend die Management-Lösung so zu konfigurieren, dass der Missbrauch von "gültigen" SSIDs erkannt wird. Weiterhin sollten Deauthentication Broadcast Pakete erkannt werden.

Zu 3) Thema Zertifizierung
Nein, es gibt keine Regelung im Rahmen der Zertifizierung, die die es erfordert, eine solche Funktion einzusetzen, um die Zertifizierung zu erhalten.

Zu 4) Nein, es ist nicht mit dem Entzug einer Zertifizierungen zu rechnen, sofern eine Hochschule solche Funktionen einsetzt (siehe Punkt 3).
Bezüglich rechtlicher Verpflichtungen (Verletzung anderer Gesetze) können wir Ihnen für Ihren konkreten Fall leider keine Auskunft geben. Die konkrete rechtliche Bewertung eines Einzelfalls stellt eine Rechtsberatung dar. Diese ist gem. Rechtsdienstleistungsgesetz den dort abschließend genannten Berufsgruppen vorbehalten.

Mit freundlichen Grüßen,
Im Auftrag
[redacted]
Bundesamt fuer Sicherheit
in der Informationstechnik
Service-Center
Postfach 20 03 63
53133 Bonn
E-Mail: service-center@bsi.bund.de
Tel.: +49 0800 - 2741000
Fax: +49 0800 - 274600
++++ Sind Sie schon Abonnent unseres Bürger-CERT Newsletters?

Anmeldung unter https://www.bsi-fuer-buerger.de/Buerger-CERT ++++

Von: Marcel Langner[redacted]

Gesendet: Dienstag, 10. September 2019 18:26
An: GP Poststelle <poststelle@bsi.bund.de>
Betreff: Re: Anfrage Deauthentication/Rogue AP Containment

Sehr geehrte Damen und Herren,
ich habe bisher keinerlei Rückmeldung zu meiner unten angefügten
Anfragen erhalten.

Am 30.08.2019 um 22:17 schrieb Marcel Langner:
> Sehr geehrte Damen und Herren,
>
> ich bitte um ein Stellungnahme zu einem technischen und rechtlichen
> Sachverhalt.
> Mir ist bekannt, dass es Hochschulen in Deutschland gibt, die mit der
> Begründung der Sicherheit ihres Netzes und der Servicequalität
> sogenannte Rogue AP Containment Funktionen gegen sämtliche andere WLANs
> in ihrer Umgebung einsetzen. Dadurch ist es nicht möglich ein WLAN (z.B.
> Mobiler Hotspot) auf den Geländen dieser Hochschulen zu betreiben.
> Technisch beruht die Rogue AP Containment Funktion auf Deauthentication
> Paketen, die Schwachstellen im WPA2 Protokoll ausnutzen.
>
> Meine Fragen:
> 1. Wie stehen Sie zu dieser Argumentation, dass zur Sicherheit des
> Netzes eine entsprechende Funktion genutzt werden kann.
> 2. Wie stehen Sie zu dieser Argumentation, dass für die Servicequalität
> des Netzes eine entsprechende Funktion genutzt werden kann.
> 3. Gibt es irgendeine Regelung im Rahmen Ihrer Zertifizierungen
> (ISO27001, Grundschutz usw.), die es erfordert, eine solche Funktion
> einzusetzen, um die Zertifizierung zu erhalten?
> 4. Ist mit dem Entzug einer Ihrer Zertifizierungen zu rechnen, sofern
> eine Hochschule solche Funktionen einsetzt? (z.B. Wegen Verletzung
> anderer Gesetze)
>
> Mit freundlichen Grüßen
> Marcel Langner
> Kuckucksweg 1A
> 15741 Bestensee
>