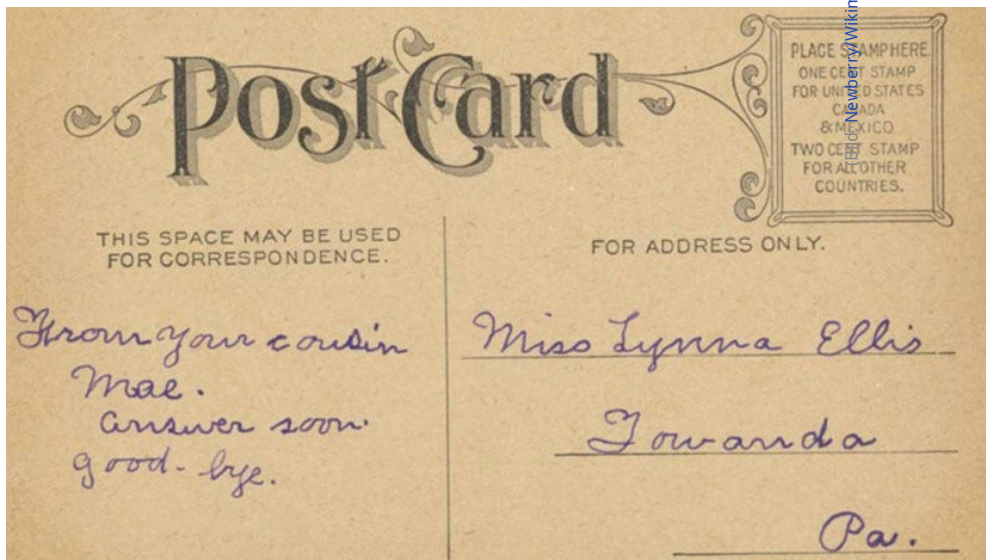


ANWALTSPOSTFACH BEA

Geheimhaltung von Nachrichten ist nicht so wichtig

Eine Sicherheitslücke im Anwaltspostfach [BeA](#) konnte nicht behoben werden, da es sich um ein grundlegendes Designproblem handelt. Die Bundesrechtsanwaltskammer hat das gelöst, indem sie das Problem wegdefinierte - mit einer abenteuerlichen Begründung: Der Schutz der Nachrichten ist nicht so wichtig, nur die Anhänge müssen geschützt sein.

10. September 2018, 14:32 Uhr Hanno Böck



Bei einer Postkarte weiß man, dass der Briefträger mitlesen kann. Aber wissen Rechtsanwälte auch, dass beim BeA die Nachrichteninhalte weniger geschützt sind?

Seit [einer Woche läuft es wieder](#), das besondere elektronische Anwaltspostfach (BeA). Doch ein schwerwiegendes Sicherheitsproblem, auf das in einem von der Bundesrechtsanwaltskammer (Brak) selbst in Auftrag gegebenen Gutachten hingewiesen wurde, besteht weiterhin. Die Brak hat uns inzwischen eine Erklärung zukommen lassen, warum sie der Ansicht ist, dass das BeA trotzdem sicher ist. Die dürfte einige Anwälte überraschen, denn sie bedeutet wohl, dass man in BeA-Nachrichten keine sensiblen Informationen übertragen darf.

Inhalt:

1. Anwaltspostfach BeA: Geheimhaltung von Nachrichten ist nicht so wichtig
2. [Keine sensiblen Informationen im Betreff und im Nachrichtentext](#)

Beim BeA werden Nachrichten verschlüsselt - und diese Verschlüsselung soll auch vor einem Innentäter schützen. So soll gewährleistet sein, dass Nachrichten auf dem BeA-Server immer nur verschlüsselt vorliegen. Auf den Servern findet eine sogenannte "Umschlüsselung" in einem Hardware-Sicherheitsmodul (HSM) statt, was auch [viel Kritik hervorgerufen hat](#), doch außerhalb dieses Sicherheitsmoduls sollten die Nachrichten nur verschlüsselt vorliegen. Auch ein Innentäter sollte demnach die Nachrichten nicht mitlesen können, solange das HSM nicht angegriffen wurde.

Webanwendung kann mitlesen

Doch hier gibt es ein grundlegendes Problem: Das BeA ist als Webanwendung realisiert, nur die eigentliche Verschlüsselung und die Kommunikation mit einer persönlichen Chipkarte sind in der lokalen BeA-Software realisiert. Somit gibt es einen geradezu trivialen Angriff: Wer die Webanwendung manipuliert, kann dort geschriebene Nachrichten nach Belieben an andere Stellen schicken.

Dieses Problem hat auch die Firma Secunet erkannt, die im Auftrag der Brak die Sicherheit des BeA untersucht hat: "Ein Innentäter kann diesen Code mit der Absicht modifizieren, Nachrichten beim Versenden unverschlüsselt in eine beliebige Richtung zu versenden", [schreibt Secunet dazu in einem Gutachten](#) und klassifiziert diese Lücke als "Kategorie A", also als besonders schwerwiegend.

Stellenmarkt

Beauftragte / Beauftragter für Informationssicherheit, Digitalisierung und E-Government

Kreis Offenbach, Dietzenbach

Mitarbeiter (m/w) für den Bereich IT-Anwenderservice

Auswärtiges Amt, Bonn

[Detailsuche](#)

Lösen ließe sich dieses Problem nur, wenn man grundlegend die Architektur des BeA neu gestaltet. Doch die Brak wollte nach den vielen Pannen der vergangenen Monate einen schnellen Neustart - eine faktische Neuentwicklung fiel damit aus. Gleichzeitig hatte [die Brak versichert](#), dass es keine Wiederinbetriebnahme des BeA geben wird, solange nicht alle Sicherheitslücken der Kategorie A behoben sind. Ein kaum auflösbarer Widerspruch.


Aus einer Lücke der Kategorie A wird eine der Kategorie B

Die Brak löste dieses Problem nun auf eine ganz besondere Art. Sie änderte einfach die Klassifizierung der Lücke - aus einem Problem der Kategorie A wurde nun eins der Kategorie B. Das wurde, wie aus einem [auf der Webseite der Rechtsanwaltskammer Berlin veröffentlichten Bericht hervorgeht](#), auf einer Präsidentenkonferenz der Bundesrechtsanwaltskammer am 27. Juni so besprochen.

Die Brak begründet die Neuklassifizierung dieser Lücke nun damit, dass die Webanwendung auf die Anhänge der Nachrichten keinen Zugriff hat. Denn diese werden durch einen speziellen Auswahldialog hinzugefügt, dessen Fenster von der BeA-Software selbst geöffnet wird. Eine Webanwendung kann dieses Fenster so nicht nachbilden.

"Schutzbedarf des Nachrichtentextes deutlich geringer"

ANZEIGE



WELTWEITER KAMPF GEGEN HÄUSLICHE GEWALT
„Beende es!": Warum jeder von uns eingreifen muss
Häusliche Gewalt ist in Lateinamerika häufig sogar eine akzeptierte Erziehungsmethode“, sagt Soledad Cardozo, Sprecherin der SOS-Kinderdörfer in Lateinamerika. » Mehr

"Nur der begleitende Nachrichtentext, welcher für Hinweise an den Empfänger genutzt werden kann, wird im Klartext mittelbar in die JavaScript-Komponente übermittelt bzw. mit ihrer Hilfe erzeugt", schreibt Brak-Pressesprecherin Stephanie Beyrich dazu. "Die relevanten Schriftsätze gegebenenfalls nebst Anlagen werden im Gegensatz dazu als Anhänge zur Nachricht im beA beigefügt. Der Schutzbedarf des begleitenden Nachrichtentextes ist hinsichtlich Vertraulichkeit aus fachlicher Sicht als deutlich geringer als der Schutzbedarf der Anhänge einzustufen. Denn die dem Mandatsgeheimnis unterliegenden Inhalte sind in den verschlüsselten Anhängen enthalten."

[Keine sensiblen Informationen im Betreff und im Nachrichtentext](#) >

1 **2** >

Themenseiten:

[BeA](#), [Efail](#), [Javascript](#), [Sicherheitslücke](#), [Verschlüsselung](#), [Server](#), [Applikationen](#), [Internet](#), [Politik/Recht](#), [Security](#)

[Zu den Kommentaren springen](#)

Erhalte täglich die wichtigsten IT-News mit unserem Newsletter:

ANMELDEN

7 Tage Schnupper-Abo

Verwandte Artikel**BEA**

Das Anwaltspostfach kommt mit Sicherheitslücken

ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Klage gegen Anwaltspostfach eingereicht

BUNDESRECHTSANWALTSKAMMER

Sicherheitsgutachten zum Anwaltspostfach enttäuscht

VERSCHLÜSSELUNG

NSA-Chiffre Speck fliegt aus dem Linux-Kernel

BEA

Anwälte wollen Ende-zu-Ende-Verschlüsselung einklagen

Meistgelesen**APPLE WATCH IM TEST**

Auch ohne EKG die beste Smartwatch

ANDROID-ERFINDER

Andy Rubin plant ein neuartiges Smartphone

PIXEL SLATE

Das Ende der Android-Tablets rückt näher

B2

Bollinger kommt Tesla mit Elektro-Pickup zuvor

WINDOWS 10

Ursache für Datenverluste durch Update gefunden

Top-Angebote

Alternate Zack Zack

(heute u. a. Aircharge Slimline Wireless Charger 9,99€, iiyama LED-Monitor 109,90€, Sankdisk 64...

Norton Security Standard 2018 | 1 Gerät | 1 Jahr
12,49€

Speicher Tiefpreiswoche bei Media Markt
(heute u. a. Sandisk 1-TB-SSD 139€, WD 4 TB HDD
extern 95€)

Sky Ticket: Start Staffel 9A von The Walking Dead
Bis Ende Dezember nur 4,99€ bezahlen (ab Januar
9,99€ mtl. ohne Kündigung)

[Weitere Angebote](#)

Folgen Sie uns**Kommentarübersicht****INAKZEPTABLE NUTZUNGSPFLICHT !**

Gunther Marko 16. Sep 2018 / [Themenstart](#)

Weg mit der Nutzungspflicht ! Und zwar unabhängig von Sicherheitsmängeln ! Diese sind...

Re: Was war jetzt am alten System falsch, so dass...

plutoniumsulfat 12. Sep 2018 / [Themenstart](#)

Es geht nicht um Sicherheit, sondern um Rechtssicherheit.

Die BRAK wollte auf Teufel komm Raus weg vom EGVP...

Mik30 11. Sep 2018 / [Themenstart](#)

Denn der war kostenlos und macht im Ergebnis genau dasselbe wie das beA jetzt. Nur mit...

Ist doch klasse

schnedan 11. Sep 2018 / [Themenstart](#)

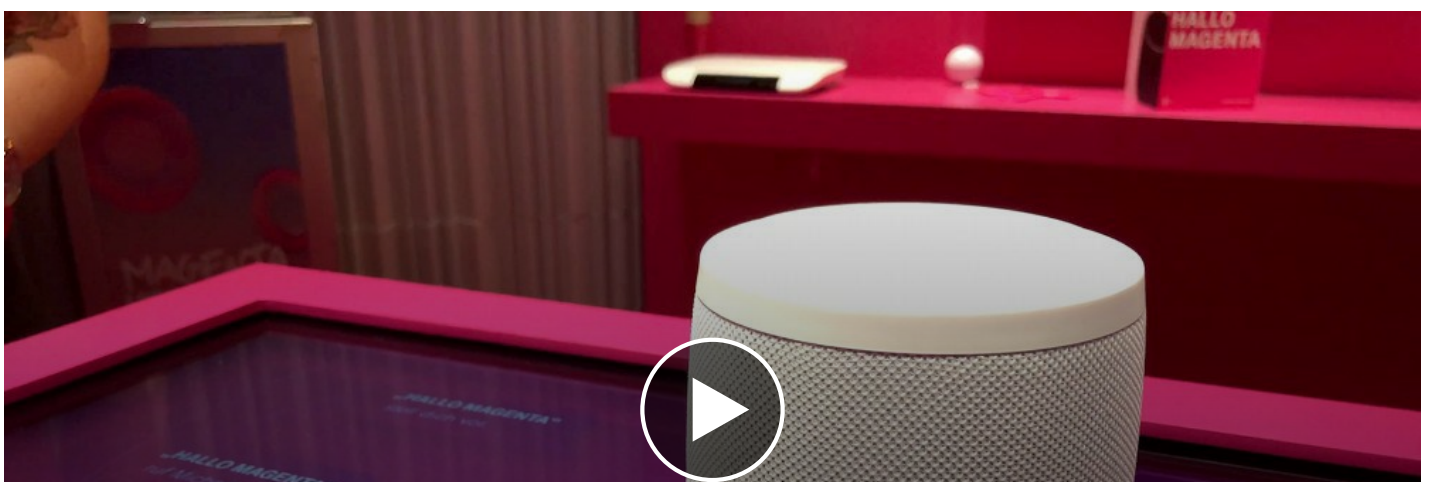
ich freu mich schon auf den nächsten unterhaltsamen Vortrag beim CCCC

Re: Ist es denn so schwer?

Mixermachine 11. Sep 2018 / [Themenstart](#)

Wie wäre es mit einem zweiten privaten Key, der ebenfalls als Versender eingetragen wird...

[Kommentieren](#)



Hallo Magenta - Präsentation auf der Ifa 2018

Auf der Ifa 2018 hat die Deutsche Telekom ihren eigenen smarten Assistenten gezeigt. Er läuft auf einem ebenfalls selbst entwickelten smarten Lautsprecher und soll zunächst trainiert werden. Telekom-Kunden können an einem Test teilnehmen und erhalten dafür den Lautsprecher kostenlos.

WLAN



WLAN-STANDARDS UMBENANNT

Ein Schritt nach vorn ist nicht weit genug

Endlich weichen die nervigen Bezeichnungen für **WLANs** chronologisch sinnvollen. Doch die Wi-Fi Alliance sollte noch einen Schritt weiter gehen.

Ein **IMHO** von Oliver Nickel

WI-FI 6 WLAN-Standards werden für besseres Verständnis umbenannt

WIFI4EU Fast 19.000 Kommunen wollen kostenloses EU-WLAN

BERLIN Bund der Steuerzahler gegen freies WLAN

Hue



LICHTVERSCHMUTZUNG

Was Philips Hue mit der Tierwelt im Garten macht

LEDs für den Garten sind energiesparend und praktisch - für Menschen und manche Fledermäuse. Für viele Tiere haben sie jedoch fatale Auswirkungen. Aber mit einigen Änderungen lässt sich die Gartenbeleuchtung so gestalten, dass sich auch Tiere wohlfühlen.

Ein Bericht von Werner Pluta

PLAY UND SIGNE Neue farbige Philips-Hue-Leuchten für indirektes Licht

SMART HOME Weitere Hue-Leuchten fürs Badezimmer vorgestellt

BADEZIMMERSPIEGEL Philips Hue kommt ins Bad

IMHO



PASSWÖRTER

Eine vernünftige Maßnahme gegen den IoT-Irrsinn

Kalifornien verabschiedet ein Gesetz, das Standardpasswörter verbietet. Das ist ein Schritt in die richtige Richtung, denn es setzt beim größten Problem von **IoT**-Geräten an und ist leicht umsetzbar.

Ein **IMHO** von Hanno Böck

RETROGAMING Maximal unnötige Minis

STREAMING Heilloses Durcheinander bei Netflix und Amazon Prime

SICHERHEIT Ein Lob für Twitter und Github

Themen	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	#	
Golem.de			Software					Mobil			Games				Security			Wissenschaft			Wirtschaft							
Tests			Browser					Akku			Spieletests				Hacker			3D-Drucker			Amazon							
PC-Hardware			Chrome					Android			Oculus Rift				Sicherheitslücke			Augmented Reality			Apple							
Prozessoren			Firefox					Cyanogenmod			Spielekonsole				TOR-Netzwerk			Automobil			Bitcoin							
Grafikkarten			Bittorrent					iOS			Playstation 4				Verschlüsselung			Cloud Computing			Facebook							
Eingabegeräte			Linux					Windows Phone			Xbox One				Chaos Computer Club			Drohne			Google							
Speichermedien			Mac OSX					Mobilfunk			Steam				Netropolitik			Künstliche Intelligenz			IBM							
4K			Windows					Oneplus					Hausautomation				Roboter			Intel								
Mini-PC			Open Source					Smartphone					Smarthome			Datenschutz		Raumfahrt			Microsoft							
Router			API					Smartwatch					LED-Lampe			DSGVO		Quantencomputer			Mozilla							
USB			Softwareentwicklung					Tablet					DIY - Do it yourself			NSA		Supercomputer			Samsung							
Digitale Fotografie			Programmiersprache					Wearable					DIY - Do it yourself			Überwachung		Virtuelle Realität			Sony							
			HTML5					Streaming					Anleitung			Vorratsdatenspeicherung					Yahoo							
			Docker					Whatsapp					Raspberry Pi			Europäische Union					Wikipedia							
																icann												