.BVT
REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
BUNDESAMT FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG

Zahl: BVT-3-CSC/20432/2015

CYBER SECURITY CENTER
HERRENGASSE 7
A-1010 WIEN
CSC@BVT.GV.AT
DVR: 0000051

Wien, am 16.10.2015

Betrifft: Betrugsversuche mittels betrügerischer E-Mails

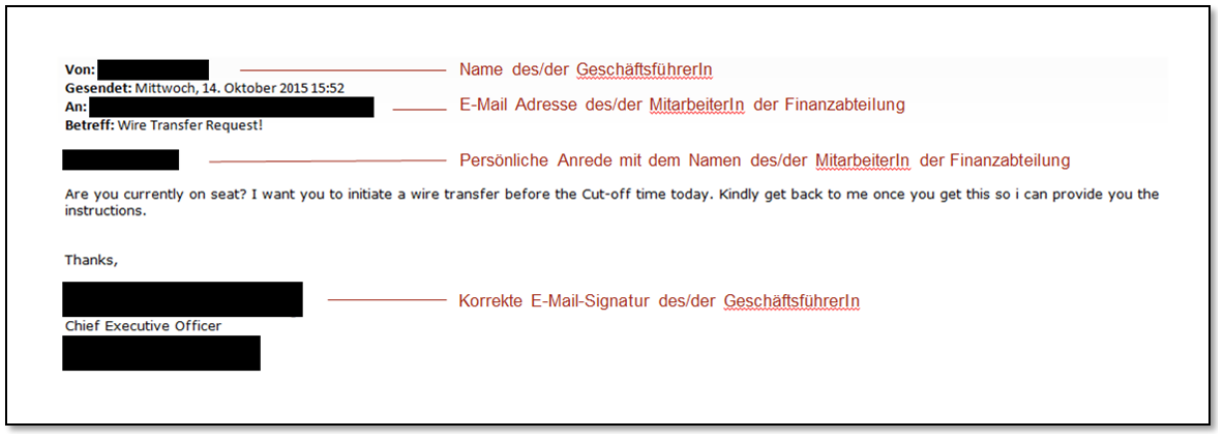
Sehr geehrte Damen und Herren,

dem Cyber Security Center (CSC) im Bundesministerium für Inneres wurden in dieser Woche mehrere Fälle von Betrugsversuchen mittels betrügerischer E-Mails gegen große Unternehmen oder Konzerne zur Kenntnis gebracht. Es liegen uns weiters konkrete Informationen vor, dass diese Betrugsmethode in jüngster Vergangenheit auch bei verschiedenen Unternehmen der österreichischen kritischen Infrastrukturen (sektorunabhängig) angewandt wurde.

Vorgehensweise:

Die uns vorliegenden Fälle zeigen eine einheitliche Vorgehensweise: Die Finanzabteilung des Unternehmens erhält eine E-Mail von der Geschäftsführung des Unternehmens, in der der/die BearbeiterIn dazu aufgefordert wird, eine dringende, unerwartete Überweisung durchzuführen. In der E-Mail wird der/die BearbeiterIn weiters aufgefordert, auf diese E-Mail zu antworten, um die dazu erforderlichen Empfängerdaten zu erhalten.

Name und E-Mail-Adresse des/der GeschäftsführerIn scheinen bei oberflächlicher Betrachtung in Ordnung. Die E-Mail ist jedoch dahingehend manipuliert, dass die Antwort nicht an die E-Mail-Adresse der Geschäftsführung, sondern direkt an den Angreifer (2015wire@raya-it.com) gesendet wird.



Da in der E-Mail hoher Zeitdruck suggeriert wird, geht der Angreifer davon aus, dass der/die MitarbeiterIn der Finanzabteilung in der Regel ohne weitere Nachfragen auf diese E-Mail antworten wird (mit der „Antworten"-Schaltfläche). Dass im „AN"-Feld zwar der Klartextname des/der GeschäftsführerIn, unmittelbar daneben allerdings die E-Mail-Adresse des Angreifers aufscheint, kann im Zeitdruck leicht übersehen werden.

In einer letzten Phase antwortet dann der Angreifer auf diese E-Mail mit der Bekanntgabe der konkreten Empfängerdaten. Betrachtet man den Mail-Header dieser E-Mail, ist die E-Mail-Adresse des Angreifers klar sichtbar.

Das Cyber Security Center empfiehlt daher dringend:

- Informieren Sie Ihre MitarbeiterInnen in potentiell gefährdeten Bereichen!

- Halten Sie Ihre MitarbeiterInnen an, sich Aufforderungen zu unerwarteten Transaktionen, insbesondere bei bisher unbekannten Empfängern oder verdächtigem Zeitdruck, nochmals persönlich oder telefonisch (nicht per E-Mail) bestätigen zu lassen!

- Achten Sie beim Verfassen einer E-Mail-Antwort (unter Verwendung der „Antworten"-Schaltfläche) stets darauf, ob es sich bei der E-Mail-Adresse des Empfängers um eine vertrauenswürdige Adresse Ihres Unternehmens handelt, bzw. ob der Empfängername und die Empfänger-E-Mail-Adresse zusammenpassen!

- Achten Sie auf die Sprache! Gegenwärtig sind solche Aufforderungen oftmals in schlechtem Englisch oder Deutsch abgefasst. Wie die Entwicklungen im Bereich von SPAM oder Phishing zeigen, ist leider gerade in diesem Bereich eine zunehmende Professionalisierung (Rechtschreibung, Grammatik) zu beobachten.

Weitere Informationen zu dieser Betrugsmethode finden Sie unter:
https://www.retarus.com/blog/de/ceo-fraud-betrueger-die-sich-als-chef-ausgeben/

Sollten Sie von einem solchen Angriff betroffen sein, bitten wir Sie, uns darüber zu informieren!

Für Rückfragen wenden Sie sich bitte an das im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung eingerichtete Cyber Security Center (csc@bvt.gv.at).

CYBER SECURITY CENTER

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

Signaturwert	qTC9Vofnju4aJ7kKLEx9rf9IT92qqZmUmI5EGhjF8UG2sytY/K6749q+0L8MfrI0qkIbrCSHHt2EFrJ6Jy355LlxHM2lUY4p0TH4y+8FsWqItnCbm6EscY9lbEYbm0WNbVZWLfh0aAouPqqr1MtCAblKtG5wjEXF0E7PdNUQdSNYMR7tauP54abRQIV39L+7ujM66lHSXepww+kyZvU0BY0ZKJqFvr4gQWtM+stVW0tnPs2FeZrzMESsCJbPaYsU6PGwoS7zGBTzSZHtbY6PIRWqGhRDF2xtHb5eYRYTzK8IljeGLYfdo9fbFmUPGQS4dXfxS3sfAQiF6ElqWxMxKw==	
	Datum/Zeit-UTC	2015-10-16T11:08:03+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1624172
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-moa-1.0
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	