Hemmnissen beim Einsatz elektronischer Verschlüsselung durch Vorgaben entgegenwirken

Ein Expertenkommentar zur BMWi-Studie

Berlin, 01. März 2018

Im Rahmen der Digitalen Strategie 2025 wurde vom Bundesministerium für Wirtschaft und Energie (BMWi) eine Studie zu den Hemmnissen beim Einsatz elektronischer Verschlüsselung in Auftrag gegeben. Die Ergebnisse wurden in dieser Woche vorgestellt. Zu den daraus entwickelten Handlungsempfehlungen zählen erwartungsgemäß „Awareness-Kampagnen", zusätzlich soll ein IT-Kompass den Verantwortlichen Orientierung geben, wo Branchenvorgaben unter Anleitung des BSI fehlen. Dass solche Vorgaben höchst effektiv sind, beweist die Energiebranche. Durch die dort flächendeckend erzwungene Verschlüsselung wird auch neuen Bedrohungen durch Big Data Analytics wirksam begegnet.

Die BMWi-Studie bestätigt wenig überraschend, dass nur getan wird, was getan werden muss. 94% der Befragten sehen Verschlüsselung als Grundsatz einer ordentlichen Geschäftsführung. Technisch möglich sei Verschlüsselung in 72% der Unternehmen. Die Sorge vor Aufwand und Kosten schiebt jedoch Investitionen auf die lange Bank. Schlechte Usability oder mangelnde Fachkenntnisse behinderten den Einsatz vorhandener Lösungen. Die Eigenmotivation, aus der Analyse der Bedrohungslagen heraus die E-Mail-Kommunikation zu verschlüsseln, ist in vielen Fällen entsprechend nicht ausreichend. Um Verschlüsselung zum Standard zu machen, muss eine gewisse Fremdmotivation über den Druck von Geschäftspartnern, Kunden und auch gesetzlichen oder branchenspezifischen Vorgaben hinzukommen.

Ein erfolgreiches Beispiel ist die Einführung der „EDI@Energy – Regelungen zum Übertragungsweg" in der Energiewirtschaft im letzten Jahr. Die gesamte elektronische Marktkommunikation der deutschen Energiewirtschaft ist nun nach aktuellsten Sicherheitsstandards verschlüsselt. Verantwortlichkeiten und Sanktionen für die möglichen Fehlerfälle wurden definiert, was dazu führt, dass es keine unverschlüsselten E-Mails zwischen Marktpartnern der Energiebranche mehr gibt. Technisch wird die Verschlüsselung über Secure Email Gateways gelöst, die automatisiert im Hintergrund arbeiten.

28% ohne Verschlüsselung, trügerische Sicherheit bei den anderen

Eine verschlüsselte Datenübertragung – zu der auch E-Mails zählen – sei laut der BMWi-Studie bei 72% der KMU und über 91% der Großunternehmen verfügbar. Dies bedeut aber nicht, dass die vorhandenen Verschlüsselungslösungen flächendeckend genutzt werden. Dies ist jedoch von großer Wichtigkeit. Die einzelne E-Mail mit brisanten, schützenswerten Inhalten zu verschlüsseln, ist nur die halbe Miete, denn was passiert mit den verbleibenden E-Mails, die das Unternehmen ungeschützt erreichen und verlassen? In Zeiten günstigen Speicherplatzes und effizienter Big-Data-Analysen ist ein mögliches Angriffsszenario, den gesamten

E-Mail-Verkehr eines Unternehmens abzufangen und strukturiert auszuwerten. Dies gewährt einen sehr intimen Einblick in Unternehmen und deren Geschäftsbeziehungen. Dieser realen Sicherheitsbedrohung kann nur mit Secure Email Gateways als hoch automatisierter Infrastrukturlösungen begegnet werden. Oft kostenfreie Einzelplatzlösungen, wie sie derzeit beim Großteil der KMU im Einsatz sind, skalieren nicht und führen tatsächlich zu hohen Aufwänden und Schulungsbedarf.

Vorgaben, die den Einsatz flächendeckender Verschlüsselungslösungen unter Verwendung sicherer Technologien fordern, wären die logische Folge der Studie. Gesetzgeber und Branchenverbände wären aufgefordert, feste Regeln zu etablieren. Stattdessen werden neue Awareness-Kampagnen ins Leben gerufen und an die Vernunft der Unternehmen appelliert, mit einem IT-Kompass als Handreichung, der die aktuelle Marktsituation nur unzureichend erfasst.

Unabhängig von der BMWi-Studie werden in Kürze Vorgaben gültig, welche die Verschlüsselung in Unternehmen forcieren. Aufgrund des IT-Sicherheitsgesetzes stehen nach der Energiebranche demnächst weitere kritische Infrastrukturen im Fokus. Ähnliche Vorgaben zur sicheren elektronischen Kommunikation werden erwartet. Auch die Europäische Datenschutz-Grundverordnung (EU DS-GVO) nimmt Unternehmen bei der Verarbeitung personenbezogener Daten in die Pflicht. Wir werden sehen, dass Regulierungen den Hemmnissen beim Einsatz elektronischer Verschlüsselung effektiv entgegenwirken.

(ca. 4.300 Zeichen)

Gesetzliche Vorgaben fördern sichere Unternehmenskommunikation
Bildnachweis: Zertificon Solutions

Zertificon-Kurzprofil

Zertificon ist seit 2004 führender Software-Hersteller im Bereich IT-Security für Unternehmen. Das unabhängige, vom Gründer geführte Unternehmen beschäftigt über 60 Mitarbeiter am Unternehmenssitz in Berlin-Neukölln. Zertificon ist Träger des „SecurITy Made in Germany“ Qualitätszeichens des Bundesverbands für IT-Sicherheit TeleTrusT.

Zertificons Z1 Lösungen ermöglichen den spontanen vertraulichen Austausch von E-Mails und großen Dateien mit Geschäftspartnern und Endkunden – zum effektiven Schutz gegen Wirtschaftsspionage und zur Erfüllung der IT-Compliance.

Z1 Lösungen bieten den höchstmöglichen Grad an Automatisierung. Anwendungsfehler bleiben bei der IT-Sicherheitssoftware aus. Sicherheitsprozesse werden hochgradig effizient und die flächendeckende Verschlüsselung wird nachhaltig und wirtschaftlich möglich – mit jedem Kontakt.

Über 20% der 100 umsatzstärksten deutschen Unternehmen haben sich bereits für Zertificon entschieden.

Zertificon Solutions GmbH
Tempelhofer Weg 62
12347 Berlin

www.zertificon.com
www.globaltrustpoint.com

Peggy Hüpenbecker
Public Relations

pr@zertificon.com
Tel.: +49 (0) 30 5900300-0
Fax: +49 (0) 30 5900300-99