DataSeCon Info 2020-02

Auswirkungen des Brexit / Bedrohung durch Ransomware

Liebe Geschäftspartnerin,
lieber Geschäftspartner,

heute möchte ich Dich gerne über die Auswirkungen des bevor stehenden Brexit und über das große Gefährdungspotential durch Ransomware informieren.

Was bedeutet der Brexit aus Sicht der DSGVO ?

Der Brexit (EU-Austritt des Vereinigten Königreichs) zum 31.01.2020 hat – nachdem es zu keinem ungeregelten Brexit gekommen ist – vorerst KEINE datenschutzrechtlichen Auswirkungen. Im Austritts-abkommen wurde eine 11-monatige Übergangsfrist vereinbart, während der das Vereinigte Königreich noch als EU-Mitglied gilt und somit alles so bleibt, wie es ist.

Eine mögliche Verlängerung dieser Übergangsfrist um ein weiteres Jahr hat das britische Parlament aber im Zuge des Austrittsvertrags bereits ausgeschlossen.

Und nach dem 31.12.2020 ?

Es deutet alles darauf hin, dass die Europäische Kommission einen sog. Angemessenheitsbeschluss fassen wird, in dem das Vereinigte Königreich als sog. „sicheres Drittland“ definiert wird (wie es derzeit bereits Andorra, Argentinien, Kanada - nur kommerzielle Organisationen, die Färöer Inseln, Guernsey, Israel, die Isle of Man, Japan, Jersey, Neuseeland, Schweiz, Uruguay und die USA - nur bei Zertifizierung nach dem „Privacy-Shield“ sind.

Sollte dieser Angemessenheitsbeschluss nicht gefasst werden, muss das Vereinigte Königreich ab dem 01.01.2021 als sog. „unsicheres Drittland“ betrachtet werden (gleich wie z.B. Russland, China, Indien, …). Eine Datenübermittlung in unsichere Drittländer ist ohne besondere Vorkehrungen nicht erlaubt. Vielmehr muss der Verantwortliche oder Auftragsverarbeiter über geeignete Maßnahmen sicherstellen, dass die übermittelten personenbezogenen Daten ausreichend geschützt werden.

Aber erst mal gehen wir optimistischer Weise davon aus, dass es diesen Angemessenheitsbeschluss geben wird …

Ransomware

Ransomware wird von Experten als DIE Bedrohung für das Jahr 2020 angesehen. Die Ausgestaltung wird dabei immer perfider und es wird immer schwerer, Ransomware als solche zu erkennen.

> Ein sehr prominentes Beispiel für die Auswirkungen einer Ransomware Attacke ist seit Monaten das Kammergericht Berlin (entspricht unseren Oberlandesgerichten). Ende September ist dort eine Infektion mit der Ransomware Emotet und im Nachgang mit TrickBot erfolgt. Aller Wahrscheinlickeit nach über ein eMail, dies konnte aber bis heute nicht zweifelsfrei festgestellt werden.
>
> Das KG Berlin ist bis heute, 4 Monate später, nur „postalisch, per Telefon und Telefax erreichbar“, wie man auf der Infoseite berlin.de nachlesen kann.

Grund für die Infektion war einerseits veraltete Software (im ggst. Fall Windows 95) und andererseits sorgloser Umgang mit mobilen Datenträgern, die zum Datenaustausch zwischen Dienst-PC und Home-PC verwendet wurden.

Inzwischen konnte aufgrund IT-forensischer Untersuchungen auch festgestellt werden, dass nicht nur die komplette IT des KG Berlin lahmgelegt wurde, sondern auch Daten abgeflossen und somit in unberechtigte Hände gelangt sind. Zu allem Überfluss musste darüber hinaus festgestellt werden, dass die Backups entweder nicht vorhanden waren oder aber nicht für die Rücksicherung verwendet werden konnten (weil ebenfalls bereits infiziert).

Erst kürzlich hat sich ein namhaftes deutsches Autozulieferunternehmen mit der Ransomware Sodinokibi infiziert und musste daraufhin seine gesamte IT-Landschaft not-abschalten. 350 der weltweit insgesamt 3.500 Beschäftigten wurden wegen der eingeschränkten „Handlungsfähigkeit“ des Unternehmens auf Zwangsurlaub geschickt.

Das Unternehmen geht davon aus, dass es „noch Monate dauern wird, bis alles wieder planmäßig funktioniert“.

Vielleicht vorab: **einen 100%igen Schutz vor Ransomware gibt es nicht ! Nur „Bleistift und Notizblock“ sind davor sicher !**

Aber man kann durchaus Maßnahmen ergreifen, um das Risiko eines Befalls weitestgehend zu reduzieren. Dazu gehören (u.a.)

- Aktuelle Softwareversionen einsetzen
  Betriebssystem: Windows 10 UND
  Anwendungen – v.a. Office: Office 2016 und höher
- Laufende Aktualisierung der Softwarekomponenten (v.a. sicherheitsrelevante Updates)
- Einsatz von Virenscannern (ebenfalls mit laufender Aktualisierung, am besten täglich)
- Restriktiver Umgang mit bzw. wenn möglich generelles Verbot von mobilen Datenträgern
- Keine „Fremdhardware“ im Unternehmensnetz erlauben
  Private Geräte von Mitarbeitern/Mitarbeiterinnen SIND Fremdhardware,
  also auch keinen Zugang zum Unternehmens WLAN für private SmartPhones erlauben
- Regelmäßige Datensicherungen durchführen
  regelmäßige (und wenn nur stichprobenartige) Rücksicherungstests durchführen
- Bewusstseinsbildung bei den Mitarbeitern/Mitarbeiterinnen (leider DIE Schwachstellen im Zusammenhang mit dieser Art Bedrohung – es ist immer ein Mitarbeiter/eine Mitarbeiterin, die den gefährlichen Anhang öffnet, er öffnet sich nicht von selbst)
- Ausreichende Absicherung des Internetzugangs (Firewall), die ein allfälliges Nachladen von weiterer Schadsoftware verhindern kann
- Bei größeren Firmennetzwerken sind Netzwerksegmentierung und Netzwerkabschottung eine Möglichkeit, die Auswirkungen eines potenziellen Befalls zu minimieren.

Sind SmartPhones denn sicher ?

Nein, sind sie nicht !

DataSeCon Info 2020-02

Auswirkungen des Brexit / Bedrohung durch Ransomware

Die zunehmende Anzahl von SmartPhones und Tablets und der Einsatz im Unternehmen macht diese Geräte für Cyber-Kriminelle zusehends interessant.

Seit ca. 8 Monaten befindet sich z.B. die Schadsoftware „x-helper“ im Umlauf, die aktuellen Schätzungen zu Folge weltweit bereits knapp 50.000 Android Devices befallen hat. x-helper ist primär darauf ausgerichtet, den Benutzer mit (unverlangter) Werbung zu bombardieren. Es besteht aber auch die Befürchtung, dass x-helper Benutzerdaten (Benutzername/Passwort) abgreift und an die Urheber der Schadsoftware übermittelt.

Das Besondere an x-helper ist, dass eine Infektion einerseits nur schwer zu erkennen ist (kein typisches App-Icon) und es andererseits nahezu unmöglich ist, die Schadsoftware loszuwerden. Selbst nach einem „auf Werkseinstellungen zurücksetzen“ installiert sich die Schadsoftware wieder selbst.

Ich möchte hiermit verdeutlichen, dass ein angemessener Virenschutz nicht nur auf dem PC, sondern auch auf dem SmartPhone, Tablet, … inzwischen unabdingbar ist. Alle namhaften Hersteller bieten dafür entsprechende Lösungen an (auch kostenlose).

Und noch eins zum Schluss: auch Apple Geräte sind nicht immun ! Allerdings sind iPhone, iPad, Mac & Co für die Cyber-Kriminellen auf Grund des Weltmarktanteils von unter 15% (noch) kein allzu interessantes Ziel. Unabhängig davon sollte man aber auch Apple Geräte entsprechend schützen.

In diesem Sinne wünsche ich einen guten Start in den Februar !

Matthias Haidekker

DataSeCon e.U.
Unternehmensberatung
Lacknerweg 38
6380 St. Johann in Tirol

T: +43 677 62 83 86 08
E: matthias.haidekker@datasecon.eu
W: www.datasecon.eu