meeting2015

Aktuelle Stunde

IT-Sicherheit

Ransom Angriffe

hmd.system
Themen für unsere Kunden im Jahr 2016

Ransom – Software – Wie schützen Sie sich vor Erpressersoftware?

Diese Software verschlüsselt Daten auf Ihrem System und kommt per Mail in die Kanzlei. Der Aufforderung nachzugehen, eine Zahlung zu leisten, hilft nichts. Was hilft ist eine gute Datensicherung.

Die sieben Fehleinschätzungen zur Sicherheit der Daten im eigenen Unternehmen:

Nr. 1 ist der Irrtum, man selbst sei doch nicht wichtig genug
Nr. 2 Öffentliche Cloudanbieter sind leichter angreifbar
Nr. 3 Passwortstärke reicht völlig aus
Nr. 4 Antivirus und Firewall sind kugelsicher
Nr. 5 Eine Universallösung hilft gegen alles
Nr. 6 Software Updates und Patches verhindern Angriffe
Nr. 7 Fehlende Sicherheitsfunktionen helfen / Die Gefahr kommt von innen

hmd.system
Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

1. Wenn Sie merken, das Sie auf einmal keinen Zugriff mehr auf Dateien auf Ihrem Filesystem haben oder Office-Dateien nicht mehr lesbar sind.

   Schalten Sie sofort alle PC‘s und Terminal Server sofort und ohne zu zögern aus. Der Schaden der durch das Ausschalten der Geräte entsteht, steht in keinem Verhältnis zu dem Verlust von ein paar Zeilen Word oder Excel, bzw. Daten in Rechnungswesen, Orga oder sonstigen Programmen.

   Das RANSOM Verschlüsselungsprogramm wird auf einem lokalen PC oder Server ausgeführt. Damit stoppen Sie die Verbreitung sofort.

hmd.system

Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

2. Informieren Sie sofort Ihren IT-Verantwortlichen bzw. IT-Betreuer.

   Dieser soll prüfen, ob es sich um einen RANSOM Angriff handelt, bzw. die nötigen Maßnahmen zur Wiederherstellung des normalen Kanzleiablaufes einleiten.

   Sie glauben das ist übertrieben? Das liegt ganz in Ihrem Ermessen.

hmd.system
Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

3. Befragung der Mitarbeiter, wer eine komische oder nicht „Mandanten Email“ angeklickt hat.

   Hier geht es nicht darum die schuldige Person zu finden, sondern den PC oder Server der das Chaos verursacht bzw. in Gang gesetzt hat.

   Sie glauben das ist übertrieben? Das liegt ganz in Ihrem Ermessen.

hmd.system
Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

4. Einschalten der PC‘s und Terminal Server

   Steht nicht 100%ig fest, ob es sich um einen Angriff handelt, dürfen PC‘s und Terminal Server nur mit getrennter Netzwerkverbindung wieder gestartet werden. Dies ist notwendig, um zu prüfen, auf welchem PC oder Server die Schadsoftware ausgeführt wird.

   Wir empfehlen, das Netzwerkkabel, bzw. das WLAN zu deaktivieren.

   Sie glauben das ist übertrieben? Das liegt ganz in Ihrem Ermessen.

hmd.system

Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

5. Reinigung des PC‘s oder Servers

   Im Internet oder bei Ihrem Anti-Virenanbieter gibt es Tools, mit denen die Software komplett entfernt werden kann.

   Dies sollte ein Profi erledigen. Denn es gibt eine Vielzahl von Stellen im Windows Betriebssystem, an denen sich das Programm verstecken kann.

hmd.system

Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

6. Schadensfeststellung und Wiederherstellung

   Es muss sofort festgestellt werden, welche Dateien betroffen sind. Damit ist geklärt, wo der Betrieb in der Kanzlei wieder aufgenommen werden kann, bzw. welche Daten aus der Datensicherung wiederhergestellt werden müssen.

   Dies sollte in Profi machen. Unterschätzen Sie den Aufwand nicht. Eine schnelle Lösung ist meistens nicht in Sicht.

hmd.system

Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

7. Schutzmaßnahmen im Vorfeld für die Kanzlei

   Leider muss ich Ihnen sagen, das es keinen 100%igen Schutz gibt. Denn das Programm, das Ihre Dateien verschlüsselt, stellt sich nicht als „Virus“ vor.

   Es gibt aber Maßnahmen, die den Schaden eingrenzen können.

hmd.system
Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

8. Einfache Sofortmaßnahmen

- Aufklärung der Mitarbeiter, im Umgang mit Emails und fremden Datenträgern
- Aktueller Virenscanner und Spamfilter für Ihre Emailserver und Clients
- Professionelle Firewall mit Portfilterung für den Internetverkehr

- Prüfung der aktuellen Datensicherung und regelmäßige weitere Prüfungen

- Entzug der Admin-Rechte für die Benutzer auf Ihren PC‘s und Servern
- Aktivieren der Windows UAC (Benutzerkontrolle) auf allen Geräten

- Reduzierung der Dateiablage auf Ihrem Fileserver (Vorgangsverwaltung und hmd.mandant)

hmd.system

Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

9. Weitere Schutzmaßnahmen und Vorsorgemaßnahmen

- Installation eines zweiten SPAM Filters und Virenscanners für Emails
- Einführung von Black- und Whitelists für Emailabsender

- Regelmäßige Überprüfung des Systems durch externe Betreuer

- Einführung Datenschutz zur Kontrolle des Email- und Internetverkehrs
- Verbot von privaten Emails und privater Internetnutzung (Duldung ist OK)
- Verbot zur Nutzung von privaten Datenträger (USB, Mobil Phone, etc.)

hmd.system
Themen für unsere Kunden im Jahr 2016

Ransom – Angriff auf Ihre Kanzlei – Was ist sofort zu tun?

Sie glauben das brauchen Sie alles nicht und außerdem kann das Ihnen ja nicht passieren.

Na dann hoffe ich das Beste für Sie.

Gerne stellen wir Ihnen den Kontakt zu Kanzleien her, die das „Chaos“ schon hinter sich haben.