TIERARZT
wir-sind-tierarzt.de

wir-sind-tierarzt wird unterstützt von:

TVD Finanz
Partner für Tierärzte

Wie schützte ich meine Tierarzt Praxis vor Cyberattacken?

ein Merkblatt von wir sind-tierarzt.de

Ausführliche und hilfreiche Informationen hat das Bundesamt für Sicherheit in der Informationstechnik auf folgenden Seiten zusammengestellt:

- ***BSI-Startseite „Erpressersoftware“*** *(Ransomware)*
- *PDF-Download:* ***„Ransomware: Bedrohungslage, Prävention & Reaktion“*** *– Ausführliches Themenpapier des BSI zu Krypto-Trojanern mit Tips zur Vorbeugung*
- *PDF-Download:* ***Lagebericht des BSI*** *zu „Erpresser-Software“ (Stand Mai 2016)*

„Hacker erpressen Tierärzte: Trojaner verschlüsselt Praxisdaten“

Den Artikel zu diesem Faktenpapier finden Sie hier auf wir-sind-tierarzt.de

Maßnahmen bei einer Erpresser-Attacke

- **Sobald man eine Verschlüsselung bemerkt gilt: Sofort den Rechner vom Netz trennen (Kabel ziehen/WLan-Modem ausschalten), um eventuell die Weiterverbreitung (noch) zu stoppen** .
  Dann den Systemadministrator und auch den Anbieter der Praxissoftware informieren und mit ihnen die nächsten Schritte abstimmen.
- Keinen Neustart ohne Absprache versuchen!
- Daten-Forensiker können – und sollten – ermitteln, auf welchem Weg der Krypto-Trojaner die Praxis-EDV-infiziert hat? Haben sich womöglich Schadprogramme im Betriebssystem eingenistet? Ist die Datensicherung eventuell ebenfalls infiziert? Welche Daten wurden verschlüsselt oder womöglich ausgelesen/übertragen/kopiert *(Haftungsrisiken siehe unten)?* Welche Einstellungen können künftig schützen?

Praxis-Tips zur Vorbeugung

Die „Ransomware“ (ransom = englisch: Lösegeld) versteckt sich üblicherweise im Anhang von teilweise sehr professionell gefälschten persönlichen Emails (z.B. Initiativ-Bewerbungen).

- Der wichtigste Sicherheitsfaktor bei einem Cyber-Angriff ist deshalb der „Mensch“: Sich und das Praxisteam immer wieder für die Bedrohung durch Schadsoftware zu sensibilisieren ist der erste Schritt.
- Dann sollte es in der Praxis verbindliche Regeln zum Umgang mit Email-Anhängen, Links in Mails und für das Surfen im Netzt vom Praxisrechner aus geben – insbesondere folgende:

Keine ZIP-Dateien öffnen

- Verdächtig sind vor allem sogenannte ZIP-Dateien oder Dateien mit der Endung „.exe". Beide deuten auf Dateien hin, die auf dem lokalen Rechner eine Aktion „ausführen“ können. Aber auch Word-Dokumente oder neuerdings sogar PDF-Dateien können infiziert sein.
- **Deshalb gilt:** Jede Mail aufmerksam lesen – prüfen ob Absender und Inhalt „zusammenpassen“ *(Oft werden Mail-Accounts gekapert und das Adressbuch für den Versand an „Freunde“ benutzt)* – Anhänge nur öffnen wenn nötig – Links in Emails überprüfen und nur anklicken wenn nötig.

Adobe-Flash-Player abschalten
Auf infizierten Internetseiten versteckt sich der „Erpresser“ zum Beispiel in Bannern – speziell das veraltete und gefährliche Adobe-Flash-PlugIn, ein Programm zum Abspielen von Web-Videos und Animationen, sollte auf keinem Praxis-Computer mehr aktiviert sein.

Anzeige

Cyber-Versicherung schützt bei Hacker-Angriff

TVD Finanz
Partner für Tierärzte

Kontakt: Oliver Rust
0421 / 89 85 8 - 23 - oliver.rust@tvd-finanz.de

Ein speziell auf Tierarztpraxen zugeschnittenes Versicherungspaket deckt ab:

- Vermögensschäden
- Haftpflichtansprüche bei Datenklau
- Eigenschäden

Bonuspaket:

- Kostenloser Zugriff auf externe IT-Spezialisten
- vorbeugende Beratung
- Hilfe bei Krisenmanagement und Datenwiederherstellung im Schadenfall

Technische Vorbeugung gegen Datenverlust und Schadsoftware

Datensicherungskonzept

1. **Wechseldatenträger auch wirklich wechseln** – ob Festplatte oder USB-Stick, alle Sicherungsmedien müssen unbedingt täglich *(sic!)* gewechselt werden. Ideal ist ein Sicherungsmedium für jeden Wochentag, sowie eine wöchentliche und monatliche Sicherung, die längerfristig archiviert wird.
2. **Datensicherung separat aufbewahren** – die Sicherung muss physisch vom Praxisnetzwerk getrennt aufbewahrt werden. Ein Trojaner versucht alle für ihn erreichbaren Festplatten und Laufwerke zu verschlüsseln. Sicherungen des Vortages sollte also vom Netz getrennt sein.
   Eine externe Lagerung der Datenträger ist auch ein Schutz vor Feuer oder Einbruchdiebstahl.
3. **Datensicherung überprüfen** – regelmäßig testen (lassen), ob eine problemlose Rücksicherung aller Dateien noch möglich ist, oder ob Kompatibilitätsprobleme bestehen.
4. **Professionelles Datensicherungsprogramm** nutzen – für das Management der Datensicherung empfehlen Experten entsprechende Programme und qualitativ hochwertige Wechselfestplatten.

Filter einschalten

Ein intelligent verwaltetes Praxisnetzwerk verbaut oder erschwert einem Angreifer den Weg ins System, sprich:

- Email-Filter einrichten
- die Zugriffsrechte für ausführbare Dateien *(Makros)* einschränken
- Zugriffsrechte der einzelnen Arbeitsplätze und Mitarbeiter definieren und wo möglich separieren
- sicherstellen, dass niemand im Praxisalltag als „Administrator“ mit allen Zugriffsrechten im Netzwerk arbeitet – auch der Chef nicht.

Virenschutz- und Software-Updates
Eine Virenschutzsoftware, die sich regelmäßig aktualisiert, ist ein Muss für eine beruflich genutzte EDV-Anlage.
Gleiches gilt für die Programmaktualisierung: Regelmäßige Softwareupdates sind Pflicht.

Haftungsfragen

Eine wichtige Frage muss außerdem geklärt werden: Welche Daten wurden womöglich nicht nur verschlüsselt, sondern eventuell auch „gestohlen“ oder ausgelesen?
Das Schadenrisiko für ein Praxis besteht nicht nur im Datenverlust, sondern auch in datenschutzrechtlichen Haftungsfragen gegenüber ihren Kunden:

- Sind Zahlungsdaten hinterlegt *(Lastschrift/Kredit-/EC-Karte)* und mit Personendaten verknüpft *(Adressen/Geburtsdatum)*?
- Gibt es bei wertvollen Tieren *(Zuchttieren)* Befunddaten, die veröffentlicht Konsequenzen haben können?

Diese Spurensicherung muss in der Regel vor einem System-Neustart über spezielle Wege erfolgen. Auch deshalb ist externe Hilfe praktisch unverzichtbar.
Gibt es Hinweise auf gestohlene/ausgelesene Daten ist mit einem Anwalt zu klären, wie man die Kunden darüber informiert/informieren muss.

Anzeige erstatten

Erpressungsversuche sollte immer auch bei der Polizei anzeigen. Es gibt spezielle Ermittlungseinheiten für Cyberkriminalität, die ebenfalls beratend weiterhelfen, aber auch auf Informationen über die Verbreitungs(wege) der Schadsoftware angewiesen sind.