SICHERHEIT IM INTERNET FÜR DIE ARZTPRAXIS

Angelockt von der Aussicht auf Gewinne aus dem Verkauf gestohlener vertraulicher Informationen, gehen kriminelle Internet-Betrüger heutzutage dazu über, das weltweite Informations-Netz als Quelle für ihre bösartigen Handlungen zu nutzen.

Aufgrund ihrer mittlerweile ausgereiften und komplexen Techniken, dem ungemeinen Ideenreichtum und ihren gezielten, regionalen Attacken, können Internet-Bedrohungen auf vielfältige Weise den Verlust von vertraulichen Informationen (einschließlich Identitätsdiebstahl), potenzielle Kosten und Ärger, verursachen.

Die Kombination dieser hohen Risiken mit der immer weiter verbreiteten Nutzung des Internets und der Komplexität eines Sicherheitsschutzes gegen Internet-Bedrohungen, stellt die vielleicht größte Herausforderung zum Schutz von persönlichen Daten und vertraulichen Geschäftsinformationen in den letzten Jahren dar.

Viren (z.B. als Textnachricht getarnte Trojaner) und schädliche Codes erreichen die in einer Arztpraxis genutzten Computer jedoch nicht nur über E-Mails oder verseuchte Websites (also per Internetanschluss), sondern häufig über die althergebrachten klassischen „Verschmutzungswege“, wie Massenspeicher.

Waren es früher Disketten und CDs, die eine Sicherheitslücke darstellten, so kommen heute die unterschiedlichsten Abwandlungen dieser Speicherderivate zum Tragen, welche über diverse Schnittstellen wie USB, Bluetooth, Funk, Infrarot oder über einen einfachen Card-Reader angeschlossen werden. So kann zum Beispiel ein USB-Stick genauso infiziert sein, wie die Speicherkarte ihrer Digitalkamera. Es sind somit mehrere Angriffswege, auch ohne Internetanschluss, denkbar und realistisch vor denen ihr PC in der Praxis oder der zugehörige Netzwerkverbund geschützt werden müssen!

WAS KANN MAN FÜR DIE SICHERHEIT IN BEZUG AUF INTERNET TUN?

1. Einen Zweit-PC für Internetaktivitäten verwenden

Eine sehr sichere Methode ist es, wenn zwischen ihrem PC mit Internetzugang und den eigentlichen Arbeitsstationen, auf denen die Praxissoftware mit den sensiblen Patientendaten läuft, keine Verbindung besteht. Damit sind die Patientendaten physikalisch vom Internet getrennt.

2. aktuellen Virenschutz installieren

Auf alle Fälle müssen alle Arbeitsgeräte mit einem aktuellen Virenschutz ausgestattet sein! Auf eine regelmäßige Aktualisierung der Virendateien muss dabei geachtet werden!

3. Eigener Router mit Firewall

Eine sichere Lösung stellt der Schutz durch eine eigene Firewall dar, welche in der Regel auf einem Router installiert wird. Ein Router regelt den Datenverkehr zwischen dem internen Netz und dem externen Netz. Diese Lösung erfordert eine professionelle Installation!

4. Geschlossenes Netz für Ärzte

Einen guten Schutz erreicht man dann, wenn man ein eigenes „Intranet“ für Ärzte vorsieht, in dem nur Personen aus dem Gesundheitsbereich kommunizieren. Über eine zentrale Firewall kann der Schutz zum öffentlichen Internet realisiert werden.

Innerhalb des Gesundheitsnetz-Vorarlberg (GNV) bietet die Ärztekammer für Vorarlberg einen solchen gesicherten Internetzugang an. Dieser Dienst ist nur für Arztpraxen, und kann nur für einen GIN-Zugang (e-card-Leitung) gewährt werden!

Patientendaten gelten in Bezug auf den Datenschutz als sensible Daten. Es muss deshalb bei der Internetnutzung und beim Thema IT-Sicherheit ein besonderes Augenmerk darauf gelegt werden!

FORMEN DER INTERNET-BEDROHUNG.

Nachfolgend sind einige Beispiele aufgeführt, die nach verschiedenen Teilen des Lebenszyklus einer Bedrohung kategorisiert sind.

- Wie die Internetverknüpfungen geliefert werden
 - Spam, Phishing-Angriffe per E-Mail, „werden Sie schnell reich“-Betrugsversuche und alle anderen zielgerichteten E-Mails, die URLs beinhalten und den Nutzer zu einer bösartigen Internetseite führen
 - Ein manipulierter Domain Name Server oder manipulierte (gefakte) Internetseiten, die den Benutzer auf betrügerische Websites (anstatt zu den richtigen) oder Proxy-Server leiten, um entweder Informationen zu stehlen oder den Benutzer zu infizieren
 - Social Networking Sites und verschiedene andere Möglichkeiten, den Benutzer zu überlisten und zu infizieren
- Schädigung über die Website
 - Schwachstellen in Mediendateien (z.B. Bilder, Animationen, Videos und Audiodateien) bei der Wiedergabe durch den Browser, durch die bösartige Dateien eingeschleust oder heruntergeladen werden
 - ActiveX-Steuer-elemente oder unbemerkte Downloads, die den Benutzer entweder dazu zwingen Dateien herunterzuladen, um sie weiter ansehen zu können, oder automatisch eine bösartige Datei übertragen, wenn ein ungeschützter Browser verwendet wird
 - Scareware wird oft dazu benutzt, um dem Benutzer einen Virenfund vorzutäuschen, und ihn in weiterer Folge dazu ermutigt, einen Download zu dessen Beseitigung durchzuführen.
- Infektionsroutine
 - Infektion durch Anwendungen, die bösartige Dateien in ein System einschleusen
 - Häufige selbstständige Aktualisierung der Internet-Bedrohung durch Download von mehreren Code-Sätzen, um mit traditioneller Antiviren-Software nicht entdeckt werden zu können
- Schadensfunktionen nach der Infektion
 - Spyware, Trojaner oder Anwendungen, die Informationen oder Daten aus einem System stehlen und sie an Dritte versenden
 - Browser-Hilfsobjekte wie Flash-Player, Shockwave-Player, die die Resultate von Suchmaschinen manipulieren oder die Surf-gewohnheiten des Benutzers überwachen, um Informationen über die Interessen des Benutzers zu sammeln (zB. Waren oder Dienstleistungen) und Werbeanzeigen zu platzieren
 - Start von Programmcode, der ferngesteuert bösartige Aktionen ausführen kann, oder über das Internet Befehle empfangen kann

Internet-Bedrohungen nutzen typischerweise Internet-Port 80 aus, der fast ständig offen ist, um Zugang zu den Informationen, Kommunikationsmöglichkeiten und der Produktivität zu ermöglichen, die das Internet den Mitarbeitern bietet.

Malware-Autoren greifen auch zu Methoden des Social Engineering und überlisten Benutzer mit verlockenden Betreffzeilen in E-Mails wie: Urlaub, Prominente, Sport, Pornografie, Weltgeschehen und andere beliebte Themen, um dann über das Aufrufen der angepriesenen Website bösartige Codes herunter zu laden.

(... aus einem Trend Micro Whitepaper ...)