



Gemanagte IT-Sicherheitslösungen von INCAS Medical

Immer *up to date* – bspw. mit unserer IT-Sicherheitslösung Protection and Security (PaS)

Die Medien sind voll davon, Hiobsbotschaften zur Cyberattacken und Sicherheitslücken allen Ortes, soweit unsere Augen und Ohren diese überhaupt noch wahrnehmen können.

Zahlreiche Fragen kommen einem selbst hierzu in den Sinn: Wie kann ich meine Arztpraxis wasserdicht vor Datenklau und sonstigen Schädlingsprogrammen machen? Stehe ich eigentlich in der Haftung, wenn bspw. Patientendaten geklaut oder vernichtet werden? Wie kann ich als IT-Verantwortlicher innerhalb eines Krankenhauses gewährleisten, dass sich unsere IP-basierten Medizingeräte im Operationssaal nicht einfach abrupt aufgrund einer Fremdeinwirkung abschalten?

Wir von INCAS Medical können zwar keine einhundertprozentige IT-Sicherheit gewährleisten, weil es diese de facto einfach nicht gibt. Jedoch können wir durch unser langjähriges Wissen und durch unsere IT-Sicherheitslösungen dazu beitragen, ein hohes Maß an Datensicherheit zu gewährleisten. Anhand unserer Sicherheitslösung PaS können wir unterstützend zur Einhaltung der geltenden datenschutzrechtlichen Anforderungen für Ärzte, Psychotherapeuten und Betreiberorganisationen, wie Krankenhäuser, einen großen Beitrag leisten.

Unsere IT-Sicherheitslösung PaS, welche durch uns physikalisch in den Räumen unserer Kunden betrieben wird, ist einfach und verständlich aufgebaut und besteht übersichtlich aus nur zwei Modulen:

Grundmodul Basic:

Beratung: Gemeinsam definieren wir im Vorfeld mit unseren Kunden die passenden Sicherheitsanforderungen sowie alle Filter- und Transportregeln für den Datenverkehr. Dabei wird im Vorfeld u.a. festgelegt, welcher Zugriffsschutz und Sicherheitslevel für welche Anwendungen und Nutzer sinnvoll sind.

Implementierung und Betrieb: In Abhängigkeit der Komplexität nehmen wir eine Vor-Ort-Installation und den anschließenden Betrieb unseres PaS-Systems (Appliance = Hardware und eine hierauf abgestimmte Sicherheits-Software) vor. Der Datenverkehr und die E-Mail-Korrespondenz kann gegen Viren und Spam abgeschottet werden, verdächtige Webseiten gesperrt bzw. kann der Zugriff von Mitarbeitern auf unerwünschte oder kommerzielle Seiten im Internet verhindert werden. Zudem können abgesicherte Zugänge für auswärtige Nutzer über ein VPN (Virtual-Private-Network) mit angeschlossen werden.

Zusatzmodul Professional:

Zusätzlich zu Basic bieten wir über ein implementiertes Zusatzmodul eine rechtzeitige Abwehr gegen Angriffe (=Prevention) an. Hierbei überwachen und analysieren wir fortlaufend besonders auffällige Zugriffsmuster aus dem Internet. Ähnlich einer intelligenten Alarmanlage werden mit Hilfe eines zusätzlichen Intrusion-Prevention-Systems (IPS) bereits verdächtige Vorfälle zur rechtzeitigen Abwehr gegen automatisierte Angriffe umgehend gemeldet. Hierdurch können sofortige Gegenmaßnahmen eingeleitet werden.



Reporting: Welches der beiden oben aufgeführten Module auch bezogen wird, regelmäßig erstellen wir ein aktuelles Reporting in fest definierten Abständen, damit unsere Kunden bezüglich ihrer IT-Sicherheit jederzeit auf dem Laufenden bleiben. Dafür sorgen unsere Service Manager, welche unsere Kunden rund um die ganzheitliche Steuerung von PaS unterstützen.

Für ein konkretes Angebot benötigen wir bitte als Mindestangabe Ihre Einrichtungsbezeichnung und die Standort- und Kontaktdaten (Ort, Straße, Nachname, E-Mail und Telefon für evtl. Rückfragen); am besten nutzen Sie hierfür unser **[Kontaktformular]** oder lassen uns alternativ eine E-Mail an **info(at)incas-medical.de** zukommen.