Das unterschätzte Problem mit dem SIS, der Konnektor ist beweisbar ein Sicherheitsrisiko

Da die IT-Dienstleister der von gematik und BMG zertifizierten TI-Firmen gegenüber den Ärzten falsche Aussagen machen, welche die Gefahren des SIS verharmlosen, muss ich nun erneut einen Artikel schreiben.

Die Aussage, dass die Sicherheit einer Praxis nach dem Anschluss eines Konnektors nicht verschlechtert werde, ist beweisbar falsch. Das habe ich bewiesen. Wenn in einer Praxis der Konnektor parallel angeschlossen und der SIS geschaltet wird, ist die Praxis ohne Wissen des Arztes vollkommen offen. Ich habe seit Wochen bemerkt, dass der SIS bei Ärzten im parallelen Anschluss geschaltet ist, ohne Wissen der Ärzte. Das macht überhaupt keinen Sinn, da der Arzt nicht vom SIS profitieren kann und auch keine Kommunikation durch den SIS gehen sollte. Es wird aber leider so gemacht. Ich habe in Praxen bereits den Beweis erbracht, dass über diesen SIS Daten gestohlen werden können, auch wenn eine richtig konfigurierte Firewall im Netz ist. Ärzte, welche ich gewarnt habe, und die ich gebeten habe den SIS abschalten zu lassen, melden mir nun, dass sie gesagt bekommen, der SIS sei nicht geschaltet, was nachweislich gelogen ist. Bitte kontrollieren Sie am Konnektor die LED SIS. Leuchtet diese, ist der SIS geschaltet. Andere bekommen die Information: „Wenn nun -wie mir der xx Techniker erklärt hat-der Konnektor über den Router verbunden ist und danach die Firewall kommt , ist doch der SIS egal? Natürlich gehe ich davon aus dass die Firewall richtig konfiguriert ist." Das ist alles natürlich vollkommener Unsinn und ich glaube, nicht einmal der Techniker der die Aussage gemacht hat glaubt den Quatsch. Zum ersten ist die Reihenfolge falsch und auch sonst ist das Unsinn. Ich möchte daher das Thema kurz so erklären, dass die Ärzte das verstehen. Dabei bediene ich mich mancher Vergleiche, die nicht immer zu 100% ganz exakt richtig sind (IT-ler mögen mir das nachsehen) aber die auf jeden Fall das Problem für Ärzte sichtbar machen und nicht falsch sind.

Die gesamte Kommunikation basiert auf IP Adressen und Ports. Die IP Adressen sind vergleichbar mit der Adresse (Ort Strasse und Hausnummer) die Ports sind vergleichbar mit den Öffnungen im Haus (Fenster, Briefkasten, Türen usw.) Es gibt also für jeden Internetanschluss 65535 Port also Öffnungen im Haus. Der SIS stellt aber eine zweite IP Adresse nach Außen zur Verfügung also eine weite Straße und Hausnummer mit weiteren 65535 Öffnungen.

Eine Firewall ist der Wächter über die Öffnungen im Haus. Aber Sie kann nur die Kommunikation auf der ersten eigenen IP Adresse sehen. Eine Stateful Packet Inspection Firewall, die (eigentlich bis auf Sonderfälle wie Client IP Modus usw.) in (fast) jedem Router eingebaut ist, sorgt lediglich dafür, dass nicht alle Öffnungen im Haus so offen stehen, dass jeder seinen Müll rein werfen kann. Um diese geht es hier nicht. Auch hier wird vielen Ärzten gesagt, z.B. der Lancom R883+ hätte ja eine Firewall und damit seien die Ärzte sicher. Das ist nicht richtig. Eine Stateful Packet Inspection Firewall ist nicht die Art Firewall, die das Praxisnetz schützt. Wichtig sind die anderen Dienstleistungen einer Hardware-Firewall, wie z.B. die Kommunikationskontrolle! Diese sorgt dafür, dass nicht jede Information, welche sich in dem Haus befindet einfach eine Öffnung aufmachen und aus dem Haus verschwinden kann. Das kann eine Stateful Packet Inspection Firewall nicht verhindern. Dort kann jedes beliebige Informationspaket eine Öffnung im Haus öffnen und aus dem Haus verschwinden. Jeder böse Bube, der erst einmal im Haus ist (Trojaner, Viren, Malware aber auch Mitarbeiter, unbefügte Patienten usw.) können einfach Öffnungen öffnen die Informationen aus den Haus tragen.

Die richtig eingestellte Kommunikationskontrolle einer Firewall verhindert dies. Eine richtig eingerichtete FW lässt einzig die Verbindungen zu, die eindeutig gewollt sind. Beispiel: In dem Haus gibt es nur einen Briefkasten. (einen Rechner mit Mailkonfiguration) in der FW wird eine Regel eingerichtet, dass Post ausschließlich in diesen Briefkasten gelegt werden darf und auch nur aus diesem Briefkasten abgeholt werden darf und nur an die Poststelle um die Ecke geliefert werden kann. Ein Abliefern an einer anderen Poststelle wird durch die Firewall ebenfalls unterbunden. Ist die FW falsch eingerichtet, kann jeder einfach einen weiteren Briefkasten an die Hauswand schrauben und Post empfangen oder Daten an beliebige andere Server versenden. In unserem Beispiel könnten dann auf anderen Rechnern einfach z.B. SMTP eingerichtet werden und darüber Daten aus dem System auf andere Server abgezogen werden. Das ist so aber nicht zulässig!

Jetzt gibt es aber auch einen Ein-Ausgang, der nicht überwacht werden kann, der SIS. Der Geheimdienst hat heimlich in das Haus unterirdisch einen Tunnel gegraben. Dieser kann von der Firewall (dem Pförtner, der die 65535 Öffnungen überwacht) nicht gesehen werden, da es sich um einen geheimen Tunnel in das Gebäude handelt. Der VPN Tunnel namens SIS, ist ein solcher Tunnel, genauso wie der TI Tunnel. Der Tunnel (SIS) hat genau so viele Öffnungen nach draußen wie das gesamte Haus. Es sind 65535 Öffnungen wo Informationen aller Art rein und raus können, aber mit einer anderen IP Adresse. Alle Informationen die dort herein und heraus gehen können von der FW nicht gesehen werden, da diese verschlüsselt sind. Die Verschlüsselung müssen Sie sich so vorstellen, dass die Transporter, die die Daten transportieren zwar für die Firewall sichtbar sind, die Transporter haben aber alle Diplomatenkennzeichen und sind gepanzert und können nicht kontrolliert werden.

Ist nun der SIS in solch einem sonst sicheren Netzwerk geschaltet, muss ich einfach nur den Ausgang der Pakete, die ich stehlen möchte, durch den Tunnel leiten. Das ist sehr einfach. Sie wollen es ausprobieren, so geht es.

Ausführen -> „cmd" eingeben -> enter → ein schwarzes Fenster öffnet sich

Befehl Route print eingeben

Unter ständige Routen den Standardgateway heraussuchen (z.B.192.168.178.190)

Neuen Befehl eingeben: route add 0.0.0.0 mask 0.0.0.0 192.168.178.190 -> enter (Adresse ist aus dem Beispiel)

Schon können Sie alle Daten abfließen lassen. Diese beiden Befehle kann natürlich auch ein Trojaner ausführen.

Ich hoffe, das konnten nun alle verstehen.

Je mehr Sie , die Ärzte, davon verstehen, umso weniger können Sie durch die Itler hinters Licht geführt werden.

Jens Ernst (06.12.19)

Happycomputer GmbH
Alfred-Klanke-Straße 5A
58239 Schwerte