

» Mit Aveticon können wir neuen Infektionsquellen in unserem Netzwerk gelassen entgegen sehen, da sie automatisch isoliert werden und wir sie dann in aller Ruhe säubern! «

Thomas Hantel
Security und Kommunikation
Vivantes Netzwerk für Gesundheit GmbH



Vivantes Netzwerk für Gesundheit GmbH erhöht die Angriffsabwehr durch Aveticon

Ein Drittel aller Patienten in Berlin wird jedes Jahr in einer von über 100 Kliniken und Instituten von Vivantes behandelt.

Als größter kommunaler Krankenhauskonzern Deutschlands ist Vivantes heute Vorreiter einer sich im Wandel befindlichen Branche. Unter dem Dach des Vivantes Netzwerks wird Patienten die ganze Bandbreite qualitativ hochwertiger medizinischer und pflegerischer Versorgung geboten.

Zur Vivantes Netzwerk für Gesundheit GmbH gehören 9 Krankenhäuser, 12 Pflegeheime, 2 Seniorenwohnhäuser, eine ambulante Rehabilitation, Medizinische Versorgungszentren, eine ambulante Krankenpflege sowie Tochtergesellschaften für Catering, Reinigung und Wäsche.

Die Vivantes Gruppe wird bereits seit einigen Jahren von der Firma Bucker EDV mit dem Kaspersky Virenschutz betreut. Das AntiVirus System erfüllt seine Aufgaben auch so wie es soll – immer wieder tauchen jedoch Situationen auf, in denen das Endgerät alleine eine Bedrohungssituation nicht mehr handhaben kann. Das ist dann keine Frage des Virenschutz Herstellers, sondern einfach eine neue Generation Malware wie z.B. der Conficker, oder ein leichtsinniges Verhalten des Anwenders mit USB-Sticks oder gefährlichen Webseiten.

Ebenfalls seit einiger Zeit wird in der Vivantes Gruppe zudem die Netzwerkzugangskontrolle macmon eingesetzt. Die vielen Standorte mit der entsprechend verteilten Infrastruktur werden von einer zentralen Stelle aus verwaltet. Nutzt in einem Außenstandort ein Besucher oder ein Eindringling jedoch einen freien Netzwerkport, kann dies nur durch Technologien wie die von macmon erkannt und verhindert werden.

Da nun bereits alle erforderlichen Komponenten vorhanden sind, um das Geschehen auf Endgeräten zu sehen und mit einer Remotekontrolle der Switchports reagieren zu können, war Aveticon von der Firma Bucker die logische Ergänzung.

Auch wenn der Virenschutz gefährliche Situationen meldet und macmon einfach zu nutzen ist, erfolgt ein manuelles Eingreifen naturgemäß zu spät.

Mit Aveticon konnten wir die Systeme im Hause Vivantes nun so miteinander verbinden, dass, sobald Kaspersky Vorfälle meldet, macmon informiert wird.

Konkret sieht es so aus, dass, sollte auf einem Endgerät eine der folgenden Situationen eintreten, Aveticon regelbasiert reagiert und die Steuerung von macmon übernimmt:

- Objekt konnte nicht gesäubert und nicht gelöscht werden
- Eine MalWare wurde innerhalb einer bestimmten Zeitspanne eine definierte Menge mal entfernt
- Eine bestimmte MalWare (definierbar) wurde entdeckt.

Aktuell erfolgt durch Aveticon dann der Befehl an macmon, das entsprechende System physikalisch vom Netzwerk zu trennen – der Switchport wird remote heruntergefahren.

Der nächste Schritt wird lt. Vivantes nun auf jeden Fall darin bestehen, zusätzlich zu den bereits eingesetzten Komponenten, das Modul V-LAN Manager von macmon einzusetzen. Damit können die Reaktionen mit Aveticon noch granularer konfiguriert werden.

Tritt dann z.B. eine MalWare auf, die zwar erkannt, aber aktuell noch nicht automatisch entfernt werden kann, wird das System in ein Quarantäne V-LAN verschoben, um so remote zuzugreifen und das System zu säubern, anstatt in „Turnschuharbeit“ vor Ort tätig werden zu müssen.



» Die Verbindung
unseres Kaspersky
Virenschutzes mit
der Netzwerkzu-
gangskontrolle mac-
mon von Mikado
durch Aveticon war
für uns die logische
Ergänzung! «

Thomas Hantel
Security und Kommunikation
Vivantes Netzwerk für Gesund-
heit GmbH



Da Aveticon noch ganz neu ist, waren zwar die Anforderungen und die Idee klar umrissen, jedoch fehlte bisher die praktische Anwendung. Das Ressort IT der Vivantes Gruppe hat daher kurz entschlossen in die Zusammenarbeit eingewilligt und ihr großes Netzwerk mit über 7.000 Endgeräten für den ersten Einsatz zur Verfügung gestellt. Nach kurzer Installation durch die Consultants der R.Bücken EDV, lief Aveticon auf dem dafür vorgesehenen System und überwachte das AntiVirus System. Nun in einer großen Live Umgebung konnten Informationen über Performanceaufwand, Funktionalität und Reaktionsgeschwindigkeit gesammelt werden.

Der Ressourcenverbrauch war von Beginn an nicht nennenswert und stieg auch im weiteren Betrieb nicht an.

Aveticon von Bücken EDV, ist die logische Ergänzung aus Virenschutz und Netzwerkzugangskontrolle und ein Produkt der Bücken EDV.

Eine Lösung die automatisch reagiert, wenn der VirenScanner einer Bedrohung einmal nicht mehr Herr werden kann. Eine Kombination der bestehenden Lösungen, die die vorhandenen Informationen nutzt und eine automatische und effektive Maßnahme trifft war bei der Entstehung das Ziel und später das Ergebnis. Wenn das AntiVirus auf einem Endgerät meldet, dass das System verseucht ist, möchte man das betreffende System möglichst schnell finden und isolieren, um händisch eingreifen zu können.

Genau das erreichen wir durch den Einsatz und die Kombination mit der NAC-Lösung macmon. Eine Netzwerkzugangskontrolle, die in der Lage ist, Systeme physikalisch vom Netzwerk zu trennen oder in ein separates V-LAN zu verweisen, indem der genutzte Switchport abgeschaltet oder umkonfiguriert wird.

So können Infektionsquellen schnellstmöglich isoliert werden, entspannt gesäubert und wieder in Betrieb genommen werden.



Die Reaktionsgeschwindigkeit entspricht den gemeinsamen Vorstellungen – sobald das Kaspersky Management von dem Ereignis erfahren hat, wurde macmon durch Aveticon zur Reaktion angestoßen.

Die Funktionalitäten wurden im Nachgang an diese erste Installation nochmals erweitert. Da immer mehr verschiedene Bedrohungen im Umlauf sind, die auch durch die Medien bekannt werden, sollte Aveticon auch auf verschiedene Funde reagieren. Mit der aktuellen Version wurde nun also die Möglichkeit geschaffen, beliebig viele Bedingungen zu erstellen und jeweils die Reaktion zu definieren.

„Das Schutzniveau konnte beträchtlich erhöht werden und sorgt damit auch für ein ruhigeres Gewissen!“

Die R. Bücken EDV-Beratung ist ein international tätiges Unternehmen mit Schwerpunkten im Bereich der Datensicherheit, des Datenschutzes, der Netzwerktechnologie und einem Team von 30 Mitarbeitern. Unternehmen in allen Größenordnungen und allen Branchen vertrauen auf die Kompetenz, Zuverlässigkeit, Flexibilität und Erfahrung aus fast 25 Jahren Sicherheitsberatung.

Einige der Kernkompetenzen mit langjährigem, starkem Knowhow sind die Computervirenabwehr, das AV-Management und generelle IT-Sicherheit. Beratung und Konzeption zielen darauf ab, eine maßgeschneiderte Lösung zu gestalten, die jederzeit erweiterbar ist und dynamisch mit den Kunden und ihren Anforderungen mitwächst.

Neben AntiViren Lösungen betreut die R. Bücken EDV Kunden in den Bereichen Content Security, Verschlüsselung, Schnittstellenkontrolle, Data Loss Prevention, Intrusion Prevention, Schwachstellen-, Patch- und Risikomanagement. Zu Ihren langjährigen Kunden zählen namhafte Firmen wie z. B. TU Ilmenau, LOOS Deutschland GmbH, ITSC GmbH oder Peek & Cloppenburg KG.