Ein professionelles System Management für die IT sorgt für mehr Sicherheit

Never touch a running system. Wirklich?

Die Erpressungssoftware «Wanna Cry» hat es wieder einmal erschreckend deutlich gezeigt: Es gibt sie immer noch, die Server und PCs die nicht oder bloss alle Schaltjahre gepatched werden. Das kann sich bitter rächen. Beim jüngsten Hacker-Angriff waren deshalb zehntausende Rechner auf der ganzen Welt innert kürzester Zeit infiziert. Die Schäden gingen in Millionenhöhe.

Betroffen waren neben zahlreichen Spitälern auch Russlands Innenministerium und die Deutsche Bahn. In Deutschland fordert nun sogar der Staat zu Updates auf.

Sicherheitslücke schon lange bekannt

Eigentlich hätte es gar nicht dazu kommen müssen. Microsoft veröffentlichte nämlich bereits am 14. März ein Security Bulletin mit allen notwendigen Informationen und einem entsprechenden Sicherheitspatch. Es sind also gut zwei Monate verstrichen, ohne dass über eine Million gefährdeter Systeme gepatched wurden – ein gewaltiges Versäumnis. Damit wurde die Tür für die Wanna Cry Attacke weit aufgestossen. Die Unvorsichtigkeit etlicher Systembetreiber rächte sich ungemein.

Enorme Kosten und Imageschaden durch Wanna Cry

Die Schäden durch den breit angelegten Hacker-Angriff sind ausserordentlich gross. So standen – namentlich in Grossbritannien – verschiedene Spitäler praktisch still. Eingriffe konnte nicht durchgeführt werden, weil die Operateure weder ihre Arbeit vorbereiten noch im OP Zugriff zu wichtigen Patientendaten hatten. Bei den stark reduzierten Arbeiten, die ausführbar waren, musste unweigerlich zum altmodischen Papier zurückgegriffen werden. Zum Umsatzverlust, der rasch Millionenhöhe erreicht haben dürfte, kamen IT-Wiederherstellungskosten dazu. Ausserdem zeigten sich die betroffenen Spitäler gegenüber Zuweisern und potenziellen Patienten von einer sehr ungünstigen Seite – so entstand ein Imageschaden, bei dem es lange Zeit brauchen wird, ihn wieder wettzumachen.

Lösegeldforderungen nachgeben?

Bei Cyber-Kriminalität stellt sich immer die Frage, ob denn den Lösegeldforderungen nachgegeben werden solle. Wie schon frühere Fälle, beispielsweise in Nordrhein-Westfalen, gezeigt haben, sind die geforderten Summen beträchtlich. Thomas Baggenstos, VR-Präsident A. Baggenstos & Co. AG, Wallisellen, äusserst sich hierzu eindeutig: «Von Lösegeldzahlungen bei Wanna Cry-Befall ist dringend abzuraten: Erstens besteht keine Garantie, dass die Systeme nachher wieder laufen und zweitens werden damit die kriminellen Organisationen unterstützt und für künftige Angriffe gestärkt.»

Keine Geiss schleckt es jedoch weg: Betriebsausfälle, Datenverlust, aufwändige Datenwiederherstellungsaktionen und nicht zuletzt ein nicht zu unterschätzender Reputationsschaden bleiben jedoch die unangenehmen Folgen eines Befalls. Diese Kosten können schnell ein ungeahntes Ausmass annehmen. Jeder Verantwortliche wird sich auf jeden Fall mit unbequemen Fragen konfrontiert sehen und es bereuen, dass er das Patch Management nicht professionell organisiert hat.

Sünden im System Management

Leider sehen IT-Sicherheits-Experten trotz dieser absehbaren Risiken immer wieder ICT-Infrastrukturen, die nach dem Prinzip «Never touch a running system» verwaltet werden. Bloss nichts ändern oder patchen, lautet die Devise. Dies geschieht meist, weil befürchtet wird, dass nachher gewisse Software nicht mehr laufen könnte.

Überlastete Systemadministratoren, organisatorische Schwachstellen und «vergessene» Systeme sind weitere Gründe, auf die man oft stösst. Solch ungünstige Situationen können dazu führen, dass Spitäler leichte Opfer raffinierter Cyber-Krimineller werden.

Managed Services als Lösung

Aufgaben, die eine Organisation nicht professionell erbringen kann oder will, werden am besten an Spezialisten ausgelagert. Dadurch werden Kapazitäten für andere, wichtigere Tätigkeiten geschaffen und man muss sich nicht mehr um Stellvertretung und Abwesenheiten kümmern. Zudem ist aufgrund von klar definierten Service Level Agreements genau geregelt, was wann zu tun ist.

Mit dem System Maintenance Service von Baggenstos haben Gesundheitsinstitutionen immer topaktuelle Systeme und sind gegen drohende Cyber-Attacken optimal geschützt.

Als Basis dient das Hardware Monitoring mit automatischer Fehlerqualifikation. Die Aktualisierung von Betriebssystem und Firmware von kritischen Systemkomponenten erfolgt nach genau festgelegten SLAs durch die von den Herstellern zertifizierten Fachleute bei Baggenstos. Sie legen damit den Grundstein für das einwandfreie Funktionieren der ICT-Infrastruktur ihrer Kunden und beugen Störungen und Datenverlust vor.

Jetzt handeln und für mehr Sicherheit sorgen

Die Kosten eines professionelle System Managements sind klar kalkulierbar und wahrscheinlich tiefer als viele Anwender denken. Mit klaren Angaben für eine sorgfältige Beurteilung der nötige Massnahmen erhalten Spitäler und Gesundheitsinstitutionen von Baggenstos umgehend ein Angebot, damit deren Verantwortliche bei künftigen Cyberattacken ruhig schlafen können.

Weitere Informationen

A. Baggenstos & Co. AG
IT Services and Solutions
8304 Wallisellen
Tel. 044 832 66 66
info@baggenstos.ch
www.baggenstos.ch