Compliance und IT-Security endlich transparent – dank neuem Tool am Helpdesk

IT-Security am Service-Desk – Sicherheit schon an der Basis

Wie kann man den First-Level-Support endlich handlungsfähig machen und zugleich vollumfängliche Transparenz über Zustand, Sicherheitsrisiken und Compliance eines Clients erhalten? Darüber hat sich der Systemintegrator Consulting4IT aus Waldbronn Gedanken gemacht und auf Grundlage der Erfahrung aus über 15 Jahren mit Service-Management-Projekten ein effektives Tool für den Service-Desk entwickelt, welches auch in Sachen Sicherheit eine gute Figur macht: First Aid Service Desk – kurz F4SD. Das erste Eigenprodukt des Unternehmens ist eine Neuheit am Markt und versteht sich als Ergänzung zu allen gängigen Service-Desk-Tools – sowohl was die Effektivität im First Level angeht als auch die Möglichkeit, Sicherheitslücken schneller erkennen zu können.

Von Linda Schmittner, Consulting4IT GmbH

Der Service-Desk: Ein heißes Eisen in Fragen des IT-Supports. Denn irgendwie scheint es nie das Gelbe vom Ei zu sein. Immer wieder wird die Software gewechselt, in der wilden Hoffnung, dass alles besser wird. Schnellere Reaktionszeiten, bessere Dokumentation, Kosteneinsparungen und hellauf begeisterte Anwender. Doch die Realität setzt den hochfliegenden Träumen von IT-Entscheidern und Admins meistens rasch ein jähes Ende. Davon abgesehen findet ein Thema neben Punkten wie Kosteneffizienz und Reaktionszeiten oftmals viel zu wenig Beachtung: Security und Compliance.

Aber was ist der Grund dafür, dass die gängige Herangehensweise und etablierte wie neue Tools immer wieder scheitern? Und warum wird in Zeiten wachsender Bedrohungen durch Cyber-Kriminalität der IT-Support nicht mit ins Boot geholt und eine Software bereitgestellt, die besonders auch in Sicherheitsfragen zumindest Transparenz bietet?

Die Consulting4IT ist diesen Fragen auf den Grund gegangen und begann an der Quelle mit ihrer Ursachenforschung: im First-Level-Support. Die Ergebnisse dieser Betrachtung waren erschreckend.

Warum ein Blindflug im First-Level-Support gefährlich ist

Man stelle sich die Mitarbeiter im First-Level-Support als Piloten eines großen Flugzeugs vor. Doch sie fliegen durch dunkelste Nacht, während draußen ein Sturm tobt. Irgendwo gibt es Risse in der Außenwand, die die Maschine auseinanderzureißen drohen. Die Piloten sitzen vor schwarzen Fenstern und haben zur Orientierung nichts weiter als einige veraltete Instrumente, die alle für sich gerade genug leisten, um irgendwie den Kurs halten zu können. Doch welche Schäden es am Flugzeug gibt und wo diese sind, ist damit kaum herauszufinden. Um der Ursache ihres Sicherheitsrisikos und anderer Probleme an der Maschine also wirklich auf den Grund gehen zu können, muss einer der Piloten seinen Platz verlassen und das gesamte Flugzeug absuchen. Als er schließlich das große Leck im Laderaum entdeckt, ist es bereits zu spät. Denn in diesem Moment fegt eine heftige Windböe durch den Spalt und richtet irreparablen Schaden an. Ein Absturz ist kaum mehr zu vermeiden.

Sie finden diesen Vergleich unverhältnismäßig? Ein kleiner Abstecher an den Platz, wo alles zentral seinen Anfang nimmt, zeigt in der Regel folgendes Szenario: Eingehende Incidents und Tickets am laufenden Band, ein Telefon, das nicht stillsteht. Von allen Seiten prasseln Arbeit und Stress auf den Mitarbeiter ein, ähnlich einem täglich tobenden Sturm. Und nun stelle man sich vor, was passiert, wenn ein Hacker die Situation ausnutzt, aufgrund einer deaktivierten Firewall ohne Weiteres Zugang ins Unternehmensnetz findet und beginnt, das System lahmzulegen. Nun stehen plötzlich immer mehr Kollegen beim

First-Level-Mitarbeiter auf der Matte und wollen wissen, was los ist. Seine Werkzeuge, um der Situation Herr zu werden? Zig verschiedene Tools und Programme, mit denen er in all dem Chaos versucht, herauszufinden, was hier gerade passiert. Auch remote und an den Arbeitsplätzen direkt kommt er nicht weiter. Allerdings ist es in diesem Moment ohnehin schon zu spät. Denn schon steht der Chef vor ihm – der Angreifer hat sich mit einem höflichen Gesuch bei diesem gemeldet. Alle Daten sind gesperrt, nichts geht mehr. Die geforderte Summe: horrend.

Die Frage, die bleibt: Warum wurde nicht früher gesehen, dass das Antivirus-System auf dem PC in der Buchhaltung längst hätte upgedatet werden müssen? Und dass die Firewall ebenfalls auf einem veralteten Stand war?

Wie sichere Punktlandungen gelingen

Zugegeben, ein krasses Beispiel. Und doch durchaus realistisch, zumal es national wie international immer häufiger zu erpresserischen Hacking-Attacken auf Unternehmen und Betriebe aller Art kommt. Nun kann ein Tool im Service-Desk natürlich kein Allheilmittel für das wuchernde Übel der stetig wachsenden Cyberkriminalität darstellen. Doch es kann zumindest eines: das Risiko senken. Das Stichwort dabei lautet Transparenz. Und genau hier setzt die Consulting4IT an. Denn ihre neue Herangehensweise und der Denkansatz, einen Mehrwert für den First-Level-Support zu schaffen, führte zur ersten Eigenentwicklung des Systemintegrators, welche auch im Bereich der IT-Security Vorteile schafft: F4SD – First Aid Service Desk.

Die Software wurde als Ergänzung zu allen gängigen Helpdesk-Tools entwickelt und speziell für die Bedürfnisse des First-Level-Supports konzipiert. Diese sind im Grunde schnell umrissen: Alle nötigen Informationen zu Ursachen und Risikoquellen auf einen Blick erkennen und eine Möglichkeit haben, Incidents direkt zu lösen sowie grundlegende Sicherheitsmängel zu beheben. F4SD bietet genau das und erfüllt die beschriebenen Anforderungen auf umfassende Weise. Denn die Kumulierung von Echtzeitinformationen mittels übersichtlichem Ampelsystem zeigt Zustand und Compliance ausgewählter Clients in Sekundenschnelle – gebündelt in einem Cockpit, das die Nutzung unzähliger Zusatztools überflüssig macht. Mittels hinterlegter Quick-Actions auf PowerShell-Basis können darüber hinaus viele Standardfälle mit einem Klick sofort gelöst werden.

Das Tool First Aid Service Desk wurde speziell für die Bedürfnisse des First-Level-Supports konzipiert.

Sofern es sich um ein komplexeres Sicherheitsproblem handelt, welches an den Second-Level-Support weitergegeben werden muss, können alle Informationen übersichtlich zusammengefasst und an diesen weitergeleitet werden. Das bedeutet ein Ende des zeit- und nervenaufreibenden Ticket-Ping-Pongs im IT-Support. Vor allem anderen bedeutet es aber eine schnellere Früherkennung und die Möglichkeit, bestehende Einfallstore gegebenenfalls auch über den Second-Level rasch schließen zu können.

Dem First-Level-Support ermöglicht das Tool Klarheit und effektive Hebel zur Handlung, bei gängigen Alltagsproblemen ebenso wie bei sicherheitsrelevanten Vorfällen. Aus einem Blindflug wird ein präziser Einsatz mit perfekten Punktlandungen – ohne Lecks und irreparable Schäden an der Maschine.

Die Moral von der Geschichte

Angesichts steigender Risiken im IT-Umfeld von Unternehmen und täglicher Meldungen von Hacking-Vorfällen wird klar, wie wichtig neben einem ganzheitlichen Sicherheitskonzept bereits die Bündelung relevanter Informationen im First-Level-Support ist. Denn Informationen wie der Firewall- oder Antivirus-Status, Bitlocker-Verschlüsselungen oder der Patch-Status können direkt aufzeigen, wie compliant ein Client ist und wo Lücken im Sicherheitsnetz eines Unternehmens bestehen. Darüber hinaus können diese Risiken mit den hinterlegten Quick-Actions gegebenenfalls sogar direkt behoben werden. Das Tool bildet damit das kleine 1 x 1 der IT-Security ab, welches grundsätzlich in jedem Unternehmen vorhanden sein sollte, es aber leider nach wie vor nicht immer ist.

Die Moral der Geschichte sollte damit klar sein: Der First-Level-Support und seine Wichtigkeit – auch in Sicherheitsfragen des Unternehmens – sollten definitiv nicht unterschätzt werden. Zumindest nicht, wenn man sein Unternehmen sicher durch jeden Sturm steuern möchte. ■

Messestand Consulting4IT GmbH: Halle 7A, Stand 210