Quelle: © fotolia_ Maksim Kabakou

Outsourcing von IT-Dienstleistungen:

Chance oder Risiko?

Eine sich ständig ändernde Datenwelt, neue Systeme und Softwareversionen: Viele Unternehmen greifen immer stärker auf externe Spezialisten zurück, um mit dieser Entwicklung Schritt zu halten. Damit verbunden ist die Übertragung von Zugriffsrechten auf kritische Daten. Wie können sich Unternehmen gegen deren missbräuchliche Verwendung absichern? Ein großer deutscher Versicherungsdienstleister setzt hierfür auf das Insider-Threat-System ObserveIT.

Von Dennis Buroh, Consist Software Solutions GmbH

Privatanwender sind immer wieder erstaunt über die Flut an neuen Softwareversionen oder Betriebssystemen, die stets mit neuen Features und neuen Methoden einhergehen. Häufig hört man Freunde und Kollegen aufstöhnen angesichts dieser schnellen Abfolge von IT-Entwicklungen. Vielen fällt es schwer, hier immer mitzuhalten.

Dieses Bild aus dem privaten Sektor lässt sich ebenso auf die Entwicklung in der internationalen und, im Besonderen, in der deutschen Wirtschaft übertragen. Den allwissenden Mitarbeiter, der für sämtliche Systeme im Unternehmen ein Experte ist, gibt es schon lange nicht mehr. Um diese Entwicklung aufzufangen, ist es gang und gäbe, auf einen externen Dienstleister zurückzugreifen. Dieser ist Experte im jeweiligen Gebiet und ermöglicht der unternehmenseigenen internen IT, sich auf andere Themen zu fokussieren. Darüber hinaus dienen externe Mitarbeiter dem Unternehmen, um Arbeitsspitzen abzudecken und die interne IT oder andere Abteilungen zu unterstützen. Ohne externe

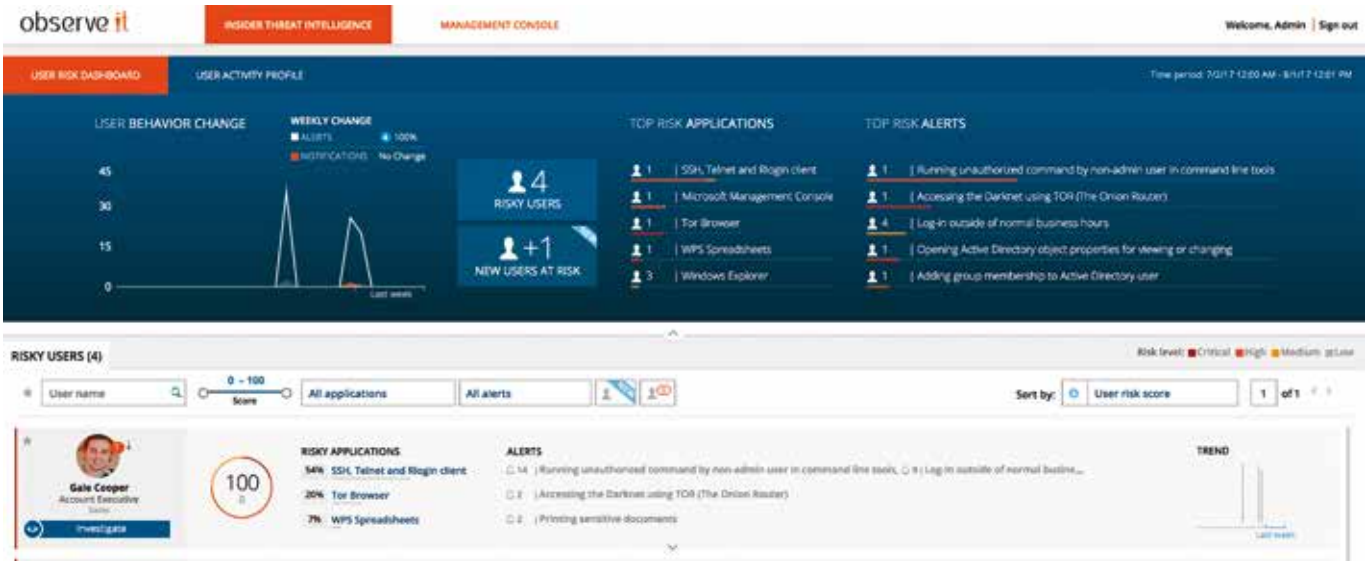

Abbildung 1: Analyse-Dashboard eines Sicherheitstools. Bild: ObserveIT

Dienstleister geht es schon lange nicht mehr in der Wirtschaft.

Der kritische Punkt

Jedoch wird für die gewünschten Tätigkeiten des externen Mitarbeiters schon lange nicht mehr nur der Dienstleister von nebenan beauftragt, sondern auch Firmen aus Spanien, Indien oder Ungarn. Die räumliche Entfernung spielt keine Rolle mehr. Durch moderne Gateways wird dem Dienstleister Zugriff auf die internen Systeme gewährt, schließlich benötigt er für seine Tätigkeiten Zugriff und Rechte auf das Firmennetz – nicht selten sogar administrative Rechte auf kritische Systeme für Updates und Wartung.

Diese Rechtevergabe ist als besonders problematisch anzusehen. Den deutschen Unternehmen ist die Gefahr hier sehr wohl bewusst: Laut Bundesamt für Informationstechnik sehen 59 Prozent hier ein großes Risiko. Auch ist es wissenschaftlich bewiesen, dass ein externer Mitarbeiter oftmals eine wesentlich geringere Hemmschwelle besitzt, Daten und Informationen des Kunden zu entwenden.

Eine Überwachung und Protokollierung von externen Mitarbeitern ist daher zwingend notwendig und auch vom Gesetzgeber gefordert. Beispielsweise steht in den Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) in AT9 (Allgemeiner Teil), dass eine wirksame Überwachung des externen Mitarbeiters gewährleistet sein muss. Weiterhin ist „die Ausführung der ausgelagerten Aktivitäten und Prozesse ordnungsgemäß zu überwachen“. Nicht nur Finanzdienstleister stehen somit in der besonderen Verpflichtung. Der Aufbau komplexer virtueller Sprungsysteme für externe Dienstleister wird daher mit einem Insider-Threat-System wie ObserveIT oder vergleichbaren Tools überwacht.

Sinnvolle Insider-Threat-Systeme

Ein großer deutscher Versicherungsdienstleister betreibt beispielsweise als Gateway-System eine Farm mit mehr als 240 virtuellen Desktopsystemen, welche direkt nach der Verwendung gelöscht und bei einer Anmeldung neu generiert werden. Durch die Neuinstallation ist ein Befall von Schadsoftware ausgeschlossen. Diese virtuelle Farm allein ermöglicht jedoch keine hundertprozentige Sicherheit. Sie kann auch nicht Prozessüberwachung und Controlling der Aktivitäten vollständig abdecken. Erst die Kombination aus einer Insider-Threat-Lösung und der Virtualisierung von Systemen garantiert einen wirksamen Schutz und das schnelle und einfache Erkennen von Anomalien. Aus diesem Grund verwendet der Versicherungsdienstleister die oben erwähnte agentenbasierte, datenschutzkonforme und datensparsame Insider-Threat-Lösung (vgl. Abbildung 1).

Solange allerdings diese hochspezialisierte Sicherheitslösung nur für externe Dienstleister eingesetzt wird, also einzig und allein für externe Mitarbeiter, die mit internen Rechten ausgestattet sind, besteht weiterhin ein nicht zu unterschätzendes Sicherheitsrisiko. Deutsche Unternehmen sehen zwar wesentlich weniger Gefahren, die von „normalen“ internen Mitarbeitern ausgehen, nach wie vor ist jedoch deren unbeabsichtigtes Fehlverhalten beispielsweise einer der Spitzenreiter bei der Bedrohung von innen heraus.

Kontakt
Consist Software Solutions GmbH
A Consist World Group Company
Falklandstr. 1–3
24159 Kiel, Germany
www.consist.de