Themenspezial

SWS COMPUTERSYSTEME

Das „Kuschel-S“ steht für „Sicherheit“. Dabei geht es sowohl um den Schutz der IT-Systeme vor Angriffen von außen als auch um ihre Ausfallsicherheit. Fotos: SWS

IT-Ausfall muss kein Notfall sein

Mit „Managed Services“, wiederkehrenden IT-Leistungen, deren Art und Umfang klar definiert werden, entlastet SWS Unternehmen bei ihrem Tagesgeschäft.

Von Stephanie Burger

REGENSBURG. Januar 2018, Frankfurt am Main: Am größten deutschen Verkehrsflughafen verspäten sich viele Flugzeuge, 23 Flüge werden komplett gestrichen. Schuld daran sind allerdings nicht die winterlichen Wetterverhältnisse, sondern ein Ausfall der IT-Systeme beim Flughafenbetreiber Fraport.

Von Systemausfällen sind nicht nur große Unternehmen betroffen: Laut einer von Techconsult im Auftrag von Hewlett-Packard durchgeführten Befragung verzeichneten 2017 mittelständische Unternehmen im Schnitt vier IT-Ausfälle pro Jahr. Jeder Ausfall kostete rund 25 000 Euro pro Stunde. Der Gesamtschaden durch nicht verfügbare IT im deutschen Mittelstand wird in der Studie mit 380 000 Euro pro Unternehmen und Jahr beziffert. IT-Ausfälle haben damit das Potenzial, ganze Unternehmen zu ruinieren.

Entlastung für den Admin

Eine umfassende Lösung dieses Problems bietet der „Managed Service“, eine große Palette von IT-Dienstleistungen, die auf Basis eines Rahmenvertrages erbracht werden. Zu den führenden Anbietern in Bayern gehört die SWS Computersysteme AG. Peter Stockinger, Leiter Managed Services bei SWS, erklärt die zentralen Vorteile für den Kunden: „Es geht um die Entlastung der Administratoren in den Unternehmen. Denn sie haben immer mehr mit internen Kernthemen zu tun, mit Updates von Betriebssystemen, mit den Anforderungen der Fachabteilungen sowie mit der Pflege ihrer Businessapplikationen.“

Hinzu komme, dass aufgrund steigender Komplexität der IT zunehmend Spezialisten für die diversen IT-Infrastruktur-Themen gefragt seien. „Selbst in großen Unternehmen kann das erforderliche Know-how kaum mehr aufgebaut werden. Im ‚Managed Service‘ hingegen stehen Fachspezialisten für einzelne Themen zur Verfügung, die wiederum als Team ein Problem von verschiedenen Perspektiven aus angehen können.“ Verschärft werde die Situation durch einen Mangel an gut ausgebildeten IT-Fachkräften. „Oft ist genau dies der Knackpunkt, an dem ein Unternehmen sich für ‚Managed Service‘ entscheidet: Ein IT-Fachmann kündigt und kann auf die Schnelle nicht ersetzt werden.“

„Managed Service“ besteht aus verschiedenen Bausteinen, die flexibel gebucht werden können. In manchen sind andere bereits enthalten. Welche Bausteine für einen Kunden sinnvoll sind, hängt von seinen internen Ressourcen ab. „Es kann bis zu einer kompletten Auslagerung gehen. Was wir aber brauchen, ist ein IT-Ansprechpartner im Unternehmen vor Ort“, sagt Stockinger.

Enge Verzahnung mit Kunden

Der „SWS Managed Service“ besteht aus fünf zentralen Bausteinen: Im Rahmen des Bausteins „Monitoring“ wird beim Kunden ein Satellit installiert, der die definierten Parameter auf ihre Erreichbarkeit und Funktion hin überwacht. „Läuft etwas aus dem Ruder, schlägt bei unserer 24-Stunden-Hotline eine Nachricht auf, die dann sofort an den Kunden weitergeht.“ Der Baustein „Health Check“ beinhaltet die zyklische Überprüfung der Geräte oder Systeme des Kunden sowie einen regelmäßigen Report über den Betriebszustand.

Im Service-Baustein „Wartung & Pflege“ werden die im Servicevertrag festgelegten Systeme und Geräte mit getesteten und vom Hersteller freigegebenen neuen Softwareversionen aktualisiert. Bucht der Kunde den Baustein „Service Desk“, so ist – anders als beim reinen Monitoring – auch die Störungsbehebung enthalten. „Der Baustein ‚Service Desk‘ ist mit verschiedenen Prioritätsstufen hinterlegt. Steht zum Beispiel die komplette IT still, gilt höchste Priorität, das heißt, nach spätestens einer Stunde schaltet sich unser Kollege online auf das Kundensystem und beginnt mit der Fehlerbehebung“, erklärt Stockinger.

Mit dem Baustein „Service Operation“ werden vertraglich festgelegte, IT-administrative Leistungen für den Kunden übernommen. Die Serviceüberführung zu SWS benötige je nach Umfang rund drei Wochen, sagt Stockinger. „Dieser Prozess ist besonders wichtig und muss deshalb von Anfang an in enger Verzahnung zwischen uns und dem Kunden erfolgen. Nachdem wir oft aus einer Notsituation heraus gerufen werden, legen wir immer sehr schnell los – damit ein Systemausfall gar nicht erst zu einem existenzgefährdenden Notfall wird.“

Christian Schreiner mit dem Schloss als Symbol für Sicherheit

„Kommandozentrale“ schützt effektiv vor Cyberangriffen

Ein Security Operations Center hilft dabei, IT-Sicherheitsvorfälle frühzeitig zu erkennen und abzuwehren.

Von Stephanie Burger

REGENSBURG. Cyberangriffe gehören inzwischen zum Unternehmensalltag: Laut Cyber-Security-Report 2017 der Wirtschaftsprüfungsgesellschaft Deloitte wird fast die Hälfte der Unternehmen wöchentlich attackiert, die überwiegende Anzahl sogar täglich. Verschärft wird die Bedrohungslage durch die zunehmende Vernetzung. Produktionsausfälle, Know-how-Verluste, Datendiebstahl mit anschließenden Erpressungsversuchen und Reputationsverlust – die Liste möglicher Folgen von Hackerangriffen ist lang.

Ein hohes Niveau an IT-Sicherheit ist deshalb unerlässlich. Als besonders wirkungsvolle Schutzmaßnahme hat sich die Einrichtung eines Security Operations Centers (SOC) erwiesen. „Im SOC laufen alle Fäden der Security zusammen, es ist eine Art Kommandozentrale, von der aus die einzelnen Maßnahmen gesteuert, überwacht, evaluiert und entsprechend angepasst werden“, erklärt Martin Kopp, SOC-Manager bei SWS. Als eines von wenigen IT-Systemhäusern in Ostbayern bietet SWS seit Frühjahr 2018 SOC als Service für seine Kunden an. „Die Angriffe werden immer raffinierter. Deshalb sollte keine Organisation mehr auf ein SOC verzichten. Der Eigenbetrieb ist jedoch nur mit einer breit aufgestellten IT-Abteilung und großem IT-Security-Know-how zu bewerkstelligen“, sagt Kopp. Selbst immer mehr große Unternehmen würden ihr SOC auslagern. „Hauptgrund ist der Fachkräftemangel, denn der Personalbedarf eines SOC für einen 24-Stunden-Betrieb ist hoch.“

Die Auslagerung an externe Experten hat vor allem den Vorteil, dass ausreichende Kapazitäten und entsprechendes Know-how zur Verfügung stehen, um IT-Sicherheitsvorfälle deutlich früher zu erkennen und abzuwehren, als es bei einer nur punktuellen Überwachung möglich ist. Das SWS Security Operations Center ruht auf fünf Säulen, die je nach Bedarf in Anspruch genommen werden können, wie Kopp erläutert. Beim „Monitoring“ – der ersten Säule – werden der Betrieb und die Verfügbarkeit von Geräten und IT-Services beobachtet sowie Anomalien als Hinweise auf mögliche Bedrohungen oder Angriffe bewertet. Die zweite Säule, das „Software-Monitoring“ zielt unter anderem darauf ab, fehlerbehaftete Softwareversionen aufzudecken. „Veraltete Software und schlechte beziehungsweise fehlerhafte Konfiguration sind die beiden größten Angriffsflächen überhaupt“, betont Kopp. Im Rahmen der dritten Säule, dem „Vulnerability-Management“, werden Schwachstellenmeldungen von Herstellern oder Sicherheitsexperten gesammelt und verfolgt, um daraus kundenindividuelle Handlungsempfehlungen abzuleiten. Die vierte Säule, die „Log-Auswertung“, ist dafür zuständig, Protokolldaten von sicherheitsrelevanten Netzwerkgeräten wie der Firewall oder Intrusion-Detection- beziehungsweise Intrusion-Prevention-Systemen (IPS) systematisch zu analysieren. „Diese Säule des SOC hebt Firewall und IPS sozusagen auf eine höhere Ebene. Denn über ihre eigentliche Funktion hinaus dient sie nun als Erkenntnisquelle, indem interne Vorgänge im Netzwerk wie Infektionen durch Schadsoftware, Informationsabflüsse oder Verletzungen von IT-Sicherheitsrichtlinien durch Mitarbeiter analysiert werden“, so Kopp. Die „Eventkorrelation“ bildet die fünfte Säule des SOC. Aufgabe dieses Tools ist es, verschiedene Quellen zusammenzuführen und daraus Korrelationen herzustellen. „Aus Einzelquellen, wie beispielsweise Logfiles oder Ereignismeldungen, entsteht auf diese Weise ein Gesamtbild, das es ermöglicht, Bedrohungsmuster zu erkennen.“

Weitere Informationen über das SWS SOC und über viele andere Trends rund um Digitalisierung und IT-Sicherheit bietet die „SWS Brain Share“ am 5. Juli in der Continental Arena. Anmeldungen dazu sind online auf www.sws.de/brain-share möglich.

Niederlassungsleiter Christian Simmel, Vorstandsvorsitzender Christian Schreiner und Vorstands-Mitglied Lothar Fesl (v. li.) auf der „BrainShare 2017“. Auch in diesem Jahr richtet SWS wieder die regionale IT-Fachmesse aus.

KONTAKT

SWS Computersysteme AG
Im Gewerbepark D 75
93059 Regensburg
Telefon: +49 (0) 941 / 20605-0
info@sws.de
www.sws.de

SWS COMPUTERSYSTEME
Member of ACP Group