Foto: Rawpixel.com I Fotolia

it-sa 2016

Treff der Security-Branche

Die it-sa boomt und zieht Jahr für Jahr eine wachsende Zahl von Ausstellern und Besuchern an. CRN hat mit Herstellern, die zum ersten Mal auf der Messe sind, über ihre Erwartungen gesprochen. Viele von ihnen wollen die Veranstaltung nutzen, um ihren Channel auszubauen – für einige ist die Messe gar der Startschuss in den indirekten Vertrieb.

Daniel Dubsky

Nicht weniger als 500 Millionen Datensätze wurden Yahoo vor zwei Jahren gestohlen, wie erst jetzt bekannt wurde. Es war vermutlich der größte Datenraub der Geschichte, aber bei weitem nicht der einzige. Allerdings illustriert er sehr schön, dass selbst Unternehmen, die allein aufgrund ihrer Größe und Bekanntheit im Fadenkreuz stehen und um ihre Gefährdung wissen, es oft nicht schaffen, sich ausreichend zu schützen. Und dass sie häufig monate- oder gar jahrelang nichts von einem Einbruch bemerken.

So oder ähnlich ergeht es auch vielen deutschen Firmen, vor allem denen aus der Industrie. Sie wurden einer Umfrage des **Bitkom** zufolge zu mehr als zwei Drittel (69 Prozent) in den vergangenen zwei Jahren zum Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage. Zum Vergleich: Über alle Wirtschaftszweige hinweg war immerhin noch gut die Hälfte (51 Prozent) von solchen Sicherheitsvorfällen betroffen. Den entstehenden Schaden beziffert der Bitkom allein für die Industrie auf 22,4 Milliarden Euro pro Jahr, für die Gesamtwirtschaft sollen es 51 Milliarden sein.

Angesichts dieser Zahlen ist es wenig verwunderlich, dass das Security-Business boomt. Schließlich müssen Unternehmen nicht nur aus Eigeninteresse ihre Systeme und Daten schützen, sondern auch um gesetzlichen Anforderungen nachzukommen. Etwa dem im vergangenen Jahr verabschiedeten IT-Sicherheitsgesetz oder der neuen EU-Datenschutzgrundverordnung, für die noch eine Übergangsfrist bis Mai 2018 läuft. Diese Entwicklung bekommt auch die **it-sa** (18. bis 20. Oktober in Nürnberg) zu spüren, die sich Jahr für Jahr über wachsende Aussteller- und Besucherzahlen freuen kann und sich längst zu einer der wichtigsten europäischen Security-Messen entwickelt hat.

Pflichttermin für Security-Spezialisten

In diesem Jahr stellt die it-sa mit über 470 Ausstellern aus 19 Ländern erneut einen Rekord auf. Bereits drei Monate vor der Messe waren die meisten Standflächen vergeben, weshalb für das nächste Jahr der Umzug in die Messehallen 9 und 10 geplant ist, die mehr Platz bieten als die aktuell genutzte Halle 12. Frank Venjakob, Executive Director der it-sa, sieht seine Messe denn auch als »die stärkste Security-Messe in Europa«, die den Vergleich mit der Infosecurity in London nicht zu scheuen brauche. Keine Frage, die it-sa ist längst ein internationaler Treff der Security-Branche.

Auch für den Channel ist die it-sa ein Pflichttermin. Systemhäuser stellen die zweitgrößte Besuchergruppe, dazu kommen viele Reseller, IT-Dienstleister und Consultingspezialisten. »Die Besucherzahlen zeigen, dass die it-sa eine zentrale Informationsplattform für den Channel ist«, fasst Venjakob zusammen (siehe Interview auf Seite 20). Das haben auch Hersteller und Distributoren erkannt und nutzen die Veranstaltung nicht nur zur Pflege bestehender Vertriebspartnerschaften, sondern auch zum Aufbau neuer.

Unter den Ausstellern der diesjährigen it-sa finden sich einige, die zum ersten Mal mit einem Stand auf der Messe vertreten sind. Ihre Ziele sind größtenteils die gleichen: ihre Marken und Produkte bekannter machen, potenzielle Kunden ansprechen und Vertriebspartner gewinnen. »Auf der it-sa gibt es keine Streuverluste«, bringt es Pia Rink von **Consistec** auf den Punkt. Man erreiche genau die gewünschte Zielgruppe.

Netzwerk-Monitoring mit Datenschutz

Der saarländische Monitoring-Spezialist Consistec (Stand 658) ist einer der it-sa-Neulinge, mit denen CRN gesprochen hat. Bislang war er vor allem auf kleinen Spezialmessen wie der Monitoring Expo unterwegs, nun strebt er nach mehr Sichtbarkeit, da er einen indirekten Vertrieb aufbaut und auf der Suche nach Partnern ist. Die können ihren Kunden mit den »Caplon« genannten Lösungen des Herstellers bei der Überwachung und Analyse von Anwendungen und Services helfen.

Consistec bietet eine Tracing-Appliance für das vollständige Erfassen von Netzwerktraffic sowie eine Lösung für das klassische Netzwerk- und Application Monitoring, die auch in zwei Spezialversionen für VoIP- und Security-Monitoring zu haben ist. »Wir entwickeln unsere Systeme in Deutschland – die sind vertrauenswürdig«, stellt der für Forschung und Entwicklung verantwortliche CEO Thomas Sinnwell heraus und erklärt, dass man viele Features implementiert habe, um Datenmissbrauch zu verhindern – schließlich würden die Appliances sehr viele Daten sammeln. Ein sehr granulares Zugriffs- und Rechtesystem soll dafür sorgen, dass Mitarbeiter oder auch IT-Dienstleister nur die für sie bestimmten Daten zu sehen bekommen. So kann der Zugriff nicht nur auf bestimmte Netzwerkbereiche beschränkt, sondern auch die Analysetiefe definiert werden – bis hinunter zu einzelnen Netzwerk-Schichten.

Für Unternehmen, deren Datenschutzanforderungen noch höher sind, hat Consistec mit »Privacy Protection« ein Modul entwickelt, das für eine Anonymisierung sorgt. Es wird auf der it-sa vorgestellt und verschleiert IP-Adressen, Telefonnummern und andere personenbezogene Daten. »Sogar einzelne Header-Informationen können verschleiert werden«, sagt Sinnwell. Wie die anderen Module des Herstellers lässt sich auch Privacy Protection einfach nachrüsten, um den Funktionsumfang der Caplon-Systeme zu erweitern.

Mit dem Aufbau eines Partnervertriebs will der ursprünglich aus dem TK-Umfeld stammende Hersteller nun neue Kundengruppen erschließen und in neue Branchen vorstoßen. Derzeit werden Schulungsmaßnahmen aufgesetzt, damit die Partner die


Foto: Consistec

»Wir entwickeln unsere Systeme in Deutschland – die sind vertrauenswürdig.«

Thomas Sinnwell, CEO Forschung und Entwicklung bei Consistec


Foto: Mateso

»Reseller sind nicht nur für den Vertrieb, sondern auch als Nutzer unserer Lösungen wichtig.«

Philip Brugger, Leitung Key Account- und Channel-Management bei Mateso


Foto: Seculution

»Unser Ansatz ist, dass auf Endpoints nur noch vertrauenswürdige Software läuft.«

Torsten Valentin, CEO von Seculution

Produkte kennenlernen und bei Kunden implementieren können. Die Produkte seien erklärungsbedürftig, sagt Sinnwell, und würden ein tiefes technisches Verständnis voraussetzen. Interessant seien sie längst nicht mehr nur für Großunternehmen, sondern mit Industrie 4.0 und der Digitalisierung von Geschäftsprozessen auch für KMU – überall dort, wo die Verfügbarkeit von Anwendungen und Services wichtig sei.

Ausgewählte Kunden will der Hersteller allerdings weiter direkt betreuen. In der Regel einen pro Branche, denn man brauche das direkte Feedback, um Zugang zu aktuellen Problemen der Kunden zu haben und die Produkte entsprechend weiterzuentwickeln, so Sinnwell. »Alles andere machen wir gerne mit Partnern.«

Passwort-Management für Unternehmen

Ähnlich wie bei Consistec sieht es bei **Mateso** (Stand 440) aus. Der Name des Unternehmens mag nicht so bekannt sein, dafür der seines Produktes. Laut Philip Brugger, Leitung Key Account- und Channel-Management, kommt »Password Safe and Repository« bei 2,5 Millionen Nutzern zum Einsatz, darunter über 10.000 Firmenkunden. Die will der Hersteller nun über Partner betreuen und baut daher einen Channel auf. Mit **Sysob** hat er sich einen erfahrenen Security-VAD ins Boot geholt, der bei der Schulung und Unterstützung der Partner hilft.

Mithilfe der Reseller sollen mehr Kunden erreicht werden. Dazu seien diese aber auch selbst eine attraktive Zielgruppe für ein Passwort-Management, da sie üblicherweise mit vielen Zugangsdaten von Kundensystemen hantieren, wie Brugger erklärt. Er sucht sowohl kleine als auch große Reseller, denn Password Safe richte sich an »Kunden vom Bäcker bis zum Großkonzern – im Prinzip an jeden, der Passwörter verwendet«. Speziell für kleine Kunden können die Partner den Serverdienst für die Passwortverwaltung auch hosten. Das sieht Brugger aber eher als Zusatzgeschäft; das eigentliche Business stecke in Beratung, Installation, Services und Support.


Foto: Efecte

»Bei amerikanischen ITSM-Anbietern liegen zumindest irgendwelche Backup-Daten immer in den USA.«

Martin Prossowski, Senior Account Manager bei Efecte

Foto: E3 CSS

»Sicherheitslösungen und Datenschutz für Cloud-Apps werden für Kunden mehr und mehr zum Thema.«

Michael Hoos, CEO von CEO E3 CSS

Auf der it-sa wird Mateso die Version 8 seines Password Safes vorstellen, an der mehr als vier Jahre gearbeitet wurde. Sie bringt neue Funktionen mit für Passwort-Resets, die Verwaltung privilegierter Benutzeraccounts, eine Discovery-Funktion für die Suche nach bestimmten Accounts im Netzwerk, ein neues Filter-System sowie zusätzliche Agenten für den Single Sign-on auf Websites und in Anwendungen. Zudem wurde die Struktur des Programms überarbeitet und setzt nun auf Gruppen und Rollen statt einfache Ordner.

Mit der Umstellung auf die Version 8 wartet auf die Mateso-Partner dann auch gleich ein attraktives Geschäft. Der Hersteller will seine Bestandskunden nur so lange weiter direkt betreuen, wie sie die alte Ausgabe 7 nutzen – und das eigentlich auch nur, weil diese eine andere Architektur hat und sich die jetzt aufgesetzten Schulungen voll auf die neue Version fokussieren. Sobald Bestandskunden auf diese umsteigen, werden sie – ebenso wie alle Neukunden – an Partner übergeben.

Die Vorstellung von Password Safe 8 soll auf der it-sa mit einer großen Release Party am Mittwochabend gefeiert werden. Darüber hinaus wird der Hersteller die Messe aber auch nutzen, um mit wichtigen Kunden zu sprechen und sie auf die kommende Betreuung durch Partner vorzubereiten. Einige hat er bereits gefunden und im September gemeinsam mit Sysob geschult. Für die während der it-sa hinzukommenden Partner sind weitere Kurse im November geplant.

Whitelisting statt Virenscanner

Schon länger indirekt unterwegs ist dagegen **Seculution** (Stand 647) aus dem nordrhein-westfälischen Werl. Der Hersteller will auf der it-sa neue Kunden und Partner gewinnen und seine Whitelisting-Lösung bekannter machen. Diese prüft beim Start von Programmen anhand des Hash-Wertes der Binärdatei, ob die Anwendung in einer Liste zugelassener Applikationen aufgeführt ist. Falls nicht, darf sie keinen Speicher allokieren und kann damit nicht ausgeführt werden. Unternehmen können auf diese Weise nicht nur genau regeln, welche Anwendungen ihre Mitarbeiter einsetzen, sondern insbesondere auch die Ausführung von Malware verhindern.

»Unser Ansatz ist, dass nur noch vertrauenswürdige Software läuft«, erklärt Seculution-CEO Torsten Valentin. Das ist zwar kein Allheilmittel, kann aber viele Angriffe verhindern, etwa wenn über Browser-Lecks eine Datei geladen wird und ausgeführt werden soll. »Wir und viele unserer Kunden haben keinen Virenscanner auf den Endpoints«, berichtet Valentin. Das spare Ressourcen und komme der Performance der Systeme zugute. Natürlich könne man auf dem Mailserver noch einen Virenscanner laufen lassen.

Interessant ist das Whitelisting aber nicht nur für den klassischen Arbeitsplatz-Rechner oder für Server, sondern auch für Systeme in der Industrie oder im Healtcare-Bereich, aus dem viele der Seculution-Kunden kommen. Dort existieren viele Systeme, die schon recht alt sind, aber nicht

CRN-Interview

»Wer Partner für gemeinsames Wachstum sucht, ist auf der it-sa richtig«

Mit CRN spricht Frank Venjakob, Executive Director der it-sa, über die Bedeutung der Messe für den Channel und die wichtigsten Themen der diesjährigen Veranstaltung.

Daniel Dubsky

CRN: *Herr Venjakob, welche Rolle spielt die it-sa aus Ihrer Sicht für den Channel?*

Frank Venjakob: Mit steigenden Ausgaben für IT-Sicherheitslösungen gewinnt das Thema IT-Security von Jahr zu Jahr an Bedeutung. Die it-sa bietet Fachhändlern, Systemhäusern und IT-Dienstleistern mit ihrem umfassenden Produkt- und Leistungsangebot eine hervorragende Übersicht zum aktuellen Marktgeschehen. Mit über 470 Ausstellern bildet die diesjährige Ausgabe den Markt noch umfassender ab und ist erneut Treffpunkt für Vertreter aus den unterschiedlichen Distributionskanälen. Wer neue Produkte oder Partnerunternehmen für gemeinsames Wachstum sucht, ist auf der it-sa richtig.

CRN: *Und wie wichtig ist der Channel für die Messe?*

Venjakob: Fast jedes zehnte Unternehmen auf der it-sa ist Distributor oder Händler. Die Besucherzahlen zeigen, dass die it-sa eine zentrale Informationsplattform für den Channel ist. Soft- und Hardware-Provider, Reseller und Großhändler, Systemhäuser, Distributoren und IT-Berater machen einen Großteil der Besucher aus.

CRN: *Mit welcher Entwicklung rechnen Sie in den nächsten Jahren?*

Venjakob: Für den Channel war die it-sa immer eine sehr attraktive Veranstaltung. Ihre große Bedeutung zeigt auch die in den letzten Jahren gewachsene Zahl der Fachbesucher aus dem Channel. Hinzu kommt das Wachstum der Messe auf zuletzt mehr als 9.000 Besucher. Letztes Jahr waren so fast 90 Prozent mehr Channel-Vertreter auf der Messe als zwei Jahre zuvor. Der Trend im Channel zur integrierten Beratungsleistung bringt es mit sich, dass sich alle Beteiligten noch mehr vernetzen, noch besser informieren und noch flexibler handeln müssen. Das gilt in Knowhow-intensiven Bereichen wie der IT-Security besonders. Insofern gehe ich auch davon aus, dass sich die positive Entwicklung der it-sa mit Blick auf den Channel fortsetzen wird.

CRN: *Was werden Ihrer Meinung nach die Trendthemen auf der diesjährigen it-sa sein?*


Frank Venjakob, Executive Director it-sa beim Veranstalter Nürnberg Messe

Foto: Nürnberg Messe

Venjakob: Das IT-Sicherheitsgesetz und der Schutz von kritischen Infrastrukturen wie Banken, Versicherungen oder Energieversorgungsunternehmen sind Themen, die Aussteller und Besucher gleichermaßen bewegen. Ebenso der Schutz vor maßgeschneiderten Angriffen und für Industrie und Produktion.

ausgetauscht oder aktualisiert werden können und sich mit der Seculution-Lösung schützen lassen. Zudem erfolge der Abgleich mit der Liste freigegebener Software binnen Millisekunden und verursache anders als Virenscanner keine Verzögerungen, die eventuell Produktionsabläufe behindern, erklärt Valentin.

Die Whitelists liegen auf einem zentralen Server, allerdings halten die Clients eine lokale Kopie vor, falls sie sich nicht zu diesem verbinden können. Was der Benutzer von der Lösung zu sehen bekommt, kann detailliert angepasst werden. So lässt sich beispielsweise festlegen, dass er einen Hinweis erhält, wenn er ein bekanntes, aber in der Firmeninfrastruktur unerwünschtes Programm zu installieren oder zu starten versucht. An anderer Stelle würden ihn Warnmeldungen womöglich nur irritieren, weshalb sie für diese Fälle deaktiviert werden können. Der Administrator erhält jedoch Alarme und umfangreiche Reports über die geblockten Anwendungen.

Neue Partner werden im Laufe der ersten Projekte, die mit Seculution gemeinsam abgewickelt werden, eingelernt – spezielle Schulungen oder Zertifizierungen gibt es nicht. Allerdings betont Valentin, es sei wichtig, dass die Partner eigene Kompetenzen aufbauen, damit sie die Lösung anpassen und bei ihren Kunden einführen können.

Zwar betreibt Seculution auch Direktgeschäft, vor allem mit größeren Kunden. Doch Valentin verspricht, man werde Partnern keine Konkurrenz machen: »Der Partner hat immer Vorrang.«

IT-Service-Management aus Finnland

Zu den internationalen Herstellern auf der it-sa zählt der finnische IT-Service-Management-Spezialist **Efecte** (Stand 379). Dieser ist in Skandinavien bereits gut etabliert und seit dem vergangenen Jahr auch auf dem deutschen Markt aktiv. Auf der it-sa will er vor allem Partner für das Identity-Management seiner ITSM-Lösung gewinnen, das seit kurzem auch separat in Deutschland vertrieben wird. Prinzipiell ist er aber an Partnern für sein gesamtes Portfolio interessiert.

Systemhäuser und Fachhändler, die beide Bereiche abdecken, hätten den Vorteil, ihren Kunden Mehrwert liefern zu können, erklärt Senior Account Manager Martin Prossowski. Sie könnten nicht nur Prozesse verbessern und automatisieren, sondern durch die Verwaltung von Benutzerrechten für Sicherheit sorgen. Wer wolle, könne sich aber auf Identity-Management oder IT-Service-Management spezialisieren – je nachdem, welche Kunden er habe und welches Wissen er bereits mitbringe. Der erste Bereich setzt vor allem Security-Knowhow voraus und ist sehr beratungsintensiv, der zweite erfordert ein tiefes Verständnis von Unternehmensprozessen. »Wir sind sehr offen, was Partner angeht, da wir noch ganz am Anfang des Vertriebsaufbaus stehen«, sagt Prossowski, der in den kommenden Monaten vor allem damit punkten will, Partner und Kunden dabei zu unterstützen, die neue EU-Datenschutzgrundverordnung einzuhalten.

Mit seinen Lösungen zielt Efecte auf Unternehmen ab 2.000 Mitarbeitern. Letztlich ist aber entscheidend wie groß deren IT ist und welche Prozesse digitalisiert sind. Diese lassen sich – unabhängig davon, ob es sich um IT-Prozesse oder Prozesse aus den Bereichen HR, Finance und Facility-Management handelt – übersichtlich darstellen und automatisieren. Das Identity-Management wird dabei beim Kunden installiert, während das IT-Service-Management als SaaS-Anwendung aus einem finnischen Rechenzentrum bereitgestellt wird. Nach Meinung von Prossowski ein Vorteil im Wettbewerb mit US-Anbietern, »bei denen zumindest irgendwelche Backup-Daten immer in den USA liegen«.

Der Account Manager sieht Efecte gut im Markt positioniert. Als kleiner Anbieter sei man nicht nur günstiger als die großen Hersteller, sondern auch flexibler, wenn es um die Anpassung und Weiterentwicklung der Produkte gehe. Zudem seien diese schnell zu implementieren und einfach zu nutzen. »Da bekommen wir sehr viel positives Feedback von Kunden und Partnern.«

Verschlüsselung für Salesforce & Co.

Wie schon im vergangenen Jahr bietet die it-sa auch 2016 eine Sonderfläche für Startups. Mit **E3 CSS** (Stand 466) ist dort etwa eine Tochter der Schweizer E3 vertreten, deren »Centraya« genannter Cloud Security Access Broker bei der Absicherung von Cloud-Anwendungen helfen soll. Centraya verschafft Unternehmen nicht nur einen Überblick über die von ihren Mitarbeitern genutzten Dienste, sondern hilft auch dabei, unberechtigte Zugriffe zu unterbinden und die gespeicherten Daten durch Verschlüsselung zu schützen.

Der Hersteller setzt dabei auf ein deterministisches Verfahren, damit sich die Daten weiterhin durchsuchen und auswerten lassen. Mit starker Verschlüsselung seien die Daten zwar noch sicherer, doch diese mache die Cloud-Dienste zu reinen Datenspeichern, merkt CEO Michael Hoos an. Um das Sicherheitsniveau anzuheben, generiere man allerdings unterschiedliche Schlüssel, etwa pro User oder pro Feld.

Da die meisten erfolgreichen Cloud-Services von US-Anbietern stammen, wächst der Bedarf an europäischen Sicherheitslösungen für diese. Hier will E3 CCS mit Centraya punkten, das in der Schweiz entwickelt wird. »Der lokale Aspekt ist in diesem Mark sehr relevant«, sagt Hoos. Zwar würden Cloud-Provider oft eigene Verschlüsselungsfunktionen haben, »aber damit bieten sie an, vor sich selbst zu schützen – das funktioniert nicht.«

Der Fokus von Centraya liegt auf den Cloud-Diensten von Salesforce und Service Now sowie Sugar CRM und Microsoft Dynamics CRM. Prinzipiell lassen sich aber auch andere Services absichern. »Wenn ein Kunde einen anderen Dienst geschützt haben möchte, können wir dafür ein Profil erstellen – das ist lediglich eine Frage der Mitarbeiterzahl und des Preises«, so Hoos.

Beim Vertrieb setzt E3 CSS ausschließlich auf Partner. Gesucht werden sowohl Reseller als auch Implementationspartner: Erstere erhalten eine Sales-Schulung und verkaufen die Lösung, während letztere auch Beratungsleistungen anbieten und die Implementierung beim Kunden übernehmen. Sie bestreiten nach einer Schulung die ersten Projekte gemeinsam mit dem Hersteller und können später von der Gold- in eine Platin-Stufe aufsteigen, wenn sie auch First-Level-Support übernehmen.

Kunden beziehen Centraya im Abonnement mit einer Abrechnung pro Monat und User für jeden geschützten Cloud-Service. Die Partner werden an den Umsätzen beteiligt – auch in den Folgejahren, wenn Kunden ihre Abos verlängern. Zudem profitieren sie vom Upsell-Potenzial, denn oft steigt die Zahl der Mitarbeiter, die Cloud-Dienste nutzen, schnell an oder es sollen neue Cloud-Dienste gesichert werden.

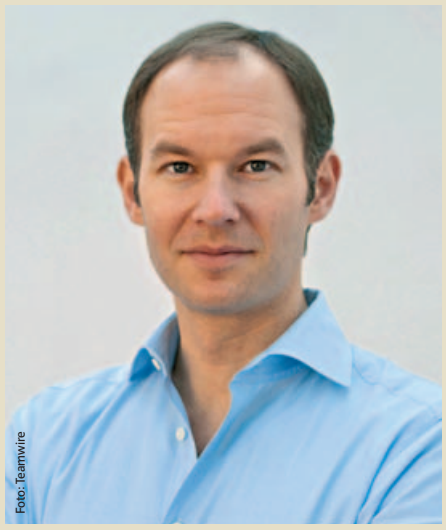
Foto: Teamwire

»E-Mail wird immer mehr zum offiziellen Kanal, über den man nach außen kommuniziert.«

Tobias Stepan, Managing Director von Teamwire


Foto: IT-Seal

»Wir simulieren Phishing-Angriffe in einer geschützten Umgebung, um Angriffspunkte aufzuspüren.«

Alex Wyllie, Mitgründer von IT-Seal

Sicheres Messaging für Unternehmen

Teamwire (Stand 466) will die Kommunikation von Unternehmen verbessern. Das Startup startete vor ein paar Jahren mit einer sicheren WhatsApp-Alternative, musste aber feststellen, dass Privatnutzer nur schwer zum Wechsel des Messengers zu bewegen sind, da meist nur ein Teil ihrer Kontakte mitwechselt. Seitdem konzentriert es sich auf Business-Kunden, bei denen eine große Nachfrage nach unternehmenstauglichen Messenger besteht, weil viele Mitarbeiter die privat genutzten Kanäle auch in der Firma einsetzen.

Teamwire ist nicht nur für Mobilgeräte mit Android, iOS und Windows Phone verfügbar, sondern auch für Desktops mit Windows, Mac OS und Linux. Die Mitarbeiter können sich somit auf all ihren Geräten mit Kollegen austauschen – die Lizenzierung erfolgt pro Benutzer, wobei dieser die App auf bis zu drei Geräten installieren kann. Der zugehörige Teamwire-Server lässt sich beim Kunden aufsetzen, kann aber auch vom IT-Dienstleister betrieben werden. Kommt beides nicht infrage, steht er über die Cloud von T-Systems bereit.

Zielgruppe des Messengers sind Unternehmen ab 250 Mitarbeitern, die hohe Datenschutz- und Compliance-Anforderungen haben. Sie erhalten mit Teamwire eine Lösung, die vollständig verschlüsselt, sich zentral verwalten lässt und ins Enterprise Mobility Management integriert. Und eine, die viele Abstimmungsprozesse verkürzt sowie Mail-Postfächer entlastet.

»Der Markt für Enterprise Messaging entsteht gerade erst und hat ein riesiges Potenzial«, sagt Tobias Stepan, Managing Director von Teamwire. Nicht nur weil sich die Kommunikation von Mail zum Chat verlagert, sondern auch weil Messenger seiner Meinung nach in den kommenden Jahren viele Unternehmensprozesse vereinfachen werden. Aus ihnen entwickle sich ein zentraler Hub, in dem alle möglichen Informationen zusammenlaufen. So könnten Reports aus Unternehmensanwendungen automatisch via Messenger an Mitarbeiter verteilt oder Genehmigungsprozesse wie eine Reisekostenabrechnung über Messenger abgewickelt werden. »E-Mail wird immer mehr zum offiziellen Kanal, über den man nach außen kommuniziert«, prognostiziert der Manager.

Für den Vertrieb sucht er Partner, die aus dem Security- oder Mobility-Umfeld kommen. Ideal seien Reseller, die regelmäßig Mobile Device Management-Lösungen einführen – sie könnten mit Teamwire den nächsten Schritt gehen und nach der Integration der Mobilgeräte in die Infrastruktur das Thema Produktivität ansprechen. Neben der Beratung, dem Deployment und dem Support seien aber auch Integrationsdienste für andere Anwendungen ein interessantes Thema. Hier entstehe ein großes Potenzial für die Partner, ist sich Stepan sicher.

Distributoren auf der it-sa

ADN: Stand 672
Also: Stand 654
Ectacom: Stand 562
Exclusive Networks: Stand 401
Infinigate: Stand 403
Jakobsoftware: Stand 217
Neox Networks: Stand 307
Prosoft: Stand 316
Sysob: Stand 226
Tech Data Mobile: Stand 668
Westcon: Stand 366
Wick Hill + Zycko: Stand 504

Phishing-Anfälligkeit auf dem Prüfstand

Noch nicht ganz so weit ist **IT-Seal** (Stand 466). Das im Rahmen des EXIST-Programms durch das Bundeswirtschaftsministerium und die EU geförderte Startup hat einen Phishing-Audit für Unternehmen entwickelt, der zur it-sa starten wird. Zunächst ist geplant, diesen direkt zu vertreiben, erst gegen Ende des kommenden Jahres will man in den indirekten Vertrieb einsteigen. Allerdings baue man bereits Kontakte zu Systemhäusern und Unternehmensberatern auf, um Feedback zu sammeln, berichtet Mitgründer Alex Wyllie.

Interessant ist die Lösung von IT-Seal für den Channel allemal, bietet sie doch einen guten Ansatzpunkt für Beratung, Schulungsdienste und Security-Services. Das Startup sammelt automatisiert im Internet, etwa auf Firmenwebsites, bei Google News, Xing und LinkedIn sowie Facebook, Informationen über das Unternehmen und seine Mitarbeiter. Die werden anschließend genutzt, um Phishing-Mails zu verschicken, um die Anfälligkeit der Mitarbeiter für derartige Attacken zu testen. Die Analysen finden auf Gruppenebene statt, damit nicht einzelne Mitarbeiter an den Pranger gestellt werden. »Wir wollen die Mitarbeiter schützen«, sagt Wyllie.

Über den Versand der Phishing-Mails werden die Mitarbeiter vorab informiert. Anfangs sind die Mails noch recht leicht zu erkennen, doch im Laufe der Zeit werden sie anhand der im Internet zusammengetragenen Informationen immer individueller. Wenn zum Beispiel eine Mail vom Chef kommt, der zu einem Meeting einlädt und die Agenda als Datei anhängt, würden schon ziemlich viele Mitarbeiter darauf hereinfallen, berichtet Wyllie. In der Regel laufe aber alles unverkrampft und ohne persönliche Schuldzuweisungen ab, denn es gehe darum, Angriffspunkte im Unternehmen aufzuspüren und zu ermitteln, in welchen Abteilungen Schulungsbedarf besteht. Die meisten Mitarbeiter würden das verstehen und hätten sogar Spaß, nach den Phishing-Mails zu fahnden.

Diesem weitgehend automatisierten Teil kann dann noch eine Security-Analyse folgen, für die IT-Seal sich die Sicherheitsrichtlinien im Unternehmen anschaut, eine Mitarbeiterbefragung zum Sicherheitsverhalten durchführt und einige Einzelinterviews führt. »Wir wollen den Unternehmen nicht nur Statistik liefern«, erklärt Wyllie. Alle Ergebnisse fließen dann letztlich in eine Auswertung ein, die Angriffspunkte auflistet und Handlungsempfehlungen gibt. »Alles basiert auf wissenschaftlicher Arbeit. Die Ergebnisse sind reproduzierbar und hängen nicht vom Auditor ab«, so der Mitgründer des Startups. ■

www.consistec.de
www.passwordsafe.de
www.seculution.de
www.efecte.com
centraya.com/de
teamwire.eu
www.it-seal.de