Die Sieger der it security Awards 2014: Versicherer Hiscox, PASA, ForgeRock und Co3

Die Sieger der it security Awards 2014: Versicherer Hiscox, PASA, ForgeRock und Co3

Das Fachmagazin it security hat heute die it security Awards 2014 auf der it-sa in Nürnberg verliehen. Hiscox hat als erster Versicherer einen Versicherungsschutz vor Hackerangriffen und Datenverlust angeboten und wurde dafür mit dem Award ausgezeichnet. Die Pallas GmbH erhielt den Award für den Schwachstellenscanner PASA. Die OpenSource-Lösung ForgeRock wurde für ihre Identity-Relationship-Management-Plattform zur Umsetzung neuer Geschäftsmodelle prämiert. Der Award für das "Innovativste Produkt des Jahres" ging an Co3, ein Management Werkzeug für den Incident Response-Prozess.
Bereits seit 2007 verleiht das Fachmagazin it security einmal jährlich die it security Awards. Eine hochkarätige Jury wählte die besten Projekte und Produkte in den Kategorien Management Security, Web/Internet Security, Identity
 Access Management und Produktinnovation des Jahres aus. Nun stehen die Preisträger der vier it security Awards 2014 fest:
Kategorie Management Security:
Hiscox: Versicherungen gegen Cyber-Risiken
In der Kategorie Management Security ging der Preis an den Versicherer Hiscox. Warum ein Versicherer? Cybercrime-Schäden kann man zwar nicht ganz verhindern, den wirtschaftlichen Schaden aber begrenzen.
Vielen kleinen und mittelständischen Unternehmen ist noch nicht bewusst, dass sie von Cyberkriminalität betroffen sein könnten - bis sie es sind. Gerade diese stehen dann oftmals vor einer existenzbedrohenden Situation und benötigen spezifische Unterstützung. Hiscox hat als erster Versicherer auf die neuen Anforderungen der Unternehmen im digitalisierten und globalisierten Zeitalter reagiert und bietet entsprechende Versicherungen gegen Cyber-Risiken. 31% der Entscheidungsträger in Unternehmen berichten von einer jährlichen Zunahme der Zwischenfälle bezüglich digitaler Daten. Cyber-Risiken rangieren auf der Rangliste der größten Risiken an vorderster Stelle. Der Leistungskatalog ist umfangreich: Präventive Krisenbetreuung/ Kostenerstattung für Sicherheitsverbesserungen nach einem Hackerangriff/ Kostenübernahme für Krisen- und PR-Beratung im Schadenfall, inklusive PR-Maßnahmen für die Wiederherstellung des Firmenimages/ Weltweiter Versicherungsschutz/ Kostenübernahme für Rechtsaufwendungen IT-Stresstest zur Überprüfung eventueller Schwachstellen als Präventionsmaßnahme/ im Schadenfall: Absicherung der Vermögensschäden, 24/7-Krisenmanagement und professionelle Kommunikationsmaßnahmen. All dies kann im Schadensfall geltend gemacht werden.
Kategorie Web/Internet Security;
PASA: Schwachstellen auf eigenen Internet-Servern selbst finden
In der Kategorie Web/Internet Security erhielt das Produkt PASA die meisten Punkte. Schwachstellen auf eigenen Internet-Servern selbst finden, ist schwierig. Oft wird auf Internet-Systemen veraltete Software eingesetzt oder versehentlich werden Ports offen stehen gelassen. PASA ist ein Service von Pallas, mit dem IT-Administratoren "von draußen" ihre Systeme überprüfen können. PASA enthält die Tools nmap und OpenVAS. Darauf aufsetzend hat die Pallas GmbH eine Betriebs- und Verwaltungsumgebung mit Web-Interface programmiert. Damit wird die regelmäßige Überprüfung auf Schwachstellen relativ einfach.
Ziel war es, die bekannten Tools nmap und OpenVAS in einer stabilen Betriebs- und Verwaltungsumgebung für IT-Administratoren in einfacher Weise verfügbar zu machen. PASA gestattet den Blick auf die Systeme von außen, so wie Angreifer die Systeme sehen. Schwachstellen auf Internet-Systemen müssen natürlich möglichst schnell geschlossen werden. Mit PASA werden die Scans automatisiert und es kann kostenlos von Externen genutzt werden. Zudem benötigen Administratoren nur rund eine Stunde Einarbeitungszeit.
Kategorie Identity
 Access Management:
ForgeRock - Identity Relationship Management für die Umsetzung neuer Geschäftsmodelle
In der Kategorie Identity
 Acess Management wurde ForgeRock ausgezeichnet. Eine der größten Hürden in diesem turbulenten Rennen um die Gunst von Kunden, Nutzern oder Bürgern stellt die Frage dar, wie mit Kundenidentitäten umgegangen werden soll. Es ist paradox: Unternehmen müssen einerseits einfachen, nahtlosen Zugriff über die verschiedenen Plattformen der Kundengeräte und Dienste hinweg bereitstellen, darunter die Cloud, das Internet der Dinge, Mobilgeräte, Kundenportale, soziale Plattformen und das Internet. Andererseits müssen sie die Sicherheit der Kunden jederzeit garantieren und gewährleisten, dass diese genau das - und nur das - bekommen, wofür sie bezahlt haben. Sie müssen also Offenheit und Restriktion zusammenbringen.
Herkömmliche Tools für die Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM) erteilen oder verweigern den Zugriff basierend auf einigen wenigen Kriterien und nur für wenige Tausend Benutzer. Typischerweise beschränken sie sich auf das Management der Identitäten von Mitarbeitern und Partnern. Unternehmen, die innovative Dienste für Kunden unterstützen möchten, können stattdessen Plattformen für Identity Relationship Management (IRM) einsetzen. Diese sehen immer auch den Aspekt der Beziehung zwischen einem Unternehmen und dem Besitzer der Identität. IRM verbessert das Identitätsmanagement dort, wo Anbieter von Legacy-Systemen es versäumt haben Innovationen hervorzubringen, und unterstützt Unternehmen bei der Entwicklung nahtloser und sicherer kundenorientierter Dienste für eine große Bandbreite von Benutzern, Anwendungen, Geräten und Dingen.
Zusammengefasst bringt der neue Ansatz in Bezug auf Identitätsmanagement Unternehmen die folgenden fünf Vorteile:
1. Beliebige Endgeräte können sich zu jeder Zeit und an jedem Ort anmelden
Unternehmen müssen eine riesige Anzahl von Geräten, Anwendungen, Benutzern und die zahlreichen Beziehungen zwischen diesen unterstützen und dabei über all ihre Berührungspunkte hinweg das gleiche Kundenerlebnis bereitstellen. Heutige Systeme für Identity Relationship Management können fast beliebige internetfähige Geräte, darunter Laptops, Touchpads und sogar Autos, sowie neue mobile und soziale Apps mit einer zentralen Sicherheitsplattform verbinden, die Identitätssynchronisierung und Einmalanmeldung (Single Sign-On, SSO) jederzeit, überall, vor Ort oder in der Cloud ermöglicht.
2. Bereitstellung kontextsensitiver Dienste
Ein Log-in ist heute nicht mehr eine einfache Ja-/Nein-Entscheidung. Mehrere Faktoren sollten darüber bestimmen, ob ein Benutzer Zugriff erhält - und falls ja, in welchem Umfang und worauf. Ein Unternehmen kann zum Beispiel sein IRM-System so einrichten, dass es je nach Situation eine zusätzliche Authentifizierungsangabe erfordert, wenn sich jemand von einem neuen Gerät oder einem anderen Land anmeldet.
Kontextsensitivität erhöht den Wert digitaler Dienste. Das In-Car-Portal von Toyota ist sich zum Beispiel immer im Klaren darüber, welcher Autobesitzer gerade auf die Plattform zugreift und wo sich Fahrer und Fahrzeug gerade befinden. Auf diese Weise kann das System Tankstellen empfehlen, einen Parkplatz finden, Echtzeit-Verkehrsinformationen bereitstellen und bei Umleitungen die Strecke neu berechnen. Andere Dienste können eine große Auswahl von Kontextdaten wie Standort, Uhrzeit, Kundendatensatz, Temperatur, Gerät und praktisch alle sonstigen Informationen nutzen, um die Interaktionen mit Benutzern individuell anzupassen.
3. Skalierung auf Tausende oder sogar Millionen von Identitäten
Da IRM-Systeme für den Zugriff auf Dienstleistungen für Kunden entwickelt wurden, bieten sie von Haus aus Kapazitäten für Tausende oder Millionen von Identitäten. Sie ermöglichen die schnelle Verifizierung dieser Identitäten sowie ihrer Berechtigungen. Immer mehr Benutzern, Geräten und Dingen wird netzwerkweit eine Identität zugeordnet. IRM hilft Unternehmen dabei, eine unkontrollierte Zunahme von Anmeldeinformationen zu vermeiden sowie einen nahtlosen und reaktionsschnellen Zugriff zu gewährleisten.
4. Offenheit und Sicherheit von Open Source
Eine gute IRM-Plattform ist als integrierte, zusammenhängende System- und Lösungsinfrastruktur konzipiert, die speziell entwickelt wurde, um komplexen Anforderungen Rechnung zu tragen. Open-Source-Lösungen sind gut geeignet, um der paradoxen Herausforderung gerecht zu werden. Sie können sowohl Offenheit als auch Sicherheit auf einer einheitlichen, hochskalierbaren Plattform bereitstellen. Und sie können mit praktisch jedem Gerät verbunden werden - auch mit verschiedenen Versionen gleichartiger Geräte. Erfahrenen Architekten zufolge sind sie zudem sicherer, weil Entwickler in der Lage sind, sicherheitsbezogene Programmfehler schneller zu identifizieren und zu beheben als bei Legacy-Closed-Source-Plattformen.
5. Schnellere Umsetzung neuer Geschäftsmodelle
Jedes Unternehmen will wachsen. Doch Unternehmen, die dafür Konsumenten ansprechen und als neue Kunden gewinnen wollen, kommen dabei oft an Grenzen, weil es aufwändig ist, hunderttausende von Kunden adäquat in der IT abzubilden. Die früher gängigen Identitäts-Lösungen lassen sich nicht in diesem Maße skalieren. Da Verbraucher stärker personalisierte Dienstleistungen verlangen, müssen sich Unternehmen Identitäten zunutze machen, um visionäre Ideen in Anwendungen zu verwandeln. Mit einem schlüssigen, ausgereiften IRM können Unternehmen schnell Lösungen bereitstellen, die mit jedem beliebigen Gerät für Millionen von Kunden funktioniert. Ein für das Internetzeitalter designtes Identitätmanagement ist also das Fundament, auf dem Unternehmen Innovationen bauen.
Unzeitgemäßes Identitätsmanagement ist für viele Unternehmen ein Wachstumshemmnis. Um dieses zu vermeiden, sind IRM-Systeme vonnöten, die mit höchster Leistung beliebige Geräte unterstützen, auf unterschiedlichste Kontexte intelligent reagieren und auf Millionen von Benutzern hochskalieren können. Damit lassen sich neue Geschäftsmodelle schneller umsetzen und ein Vorsprung im Rennen um die Gunst von Käufern erringen.
Innovativstes Produkt des Jahres
Co3 - Management Werkzeug für den Incident Response-Prozess
Als innovativstes Produkt des Jahres wählte die Jury Co3, ein Management Werkzeug für den Incident Response-Prozess.
Basierend auf einer breiten Wissensbasis,

Industriestandards und vielen länderspezifischen rechtlichen Anforderungen hat das Unternehmen Co3 rund um seinen CTO Bruce Schneier ein Werkzeug zur Unterstützung der Abläufe und Aufgaben bei Incident Response entwickelt. Das Produkt dient dabei als zentrale Kommunikationsplattform, über die offene Aufgaben je nach Art des Vorfalls verwaltet und Erkenntnisse bereitgestellt beziehungsweise ausgetauscht werden können.
Effektives Incident Response basiert auf vier Säulen: Vorbereitung, Bewertung, Management und Bericht. Co3 unterstützt diese vier kritischen Prozesse für verschiedene Arten von Sicherheitsvorfällen wie zum Beispiel Malware, Systemeinbruch, DDoS-Attacken oder Verlust vertraulicher Daten.
Für alle Arten sind die notwendigen Arbeitsschritte hinterlegt und können mit jedem Vorfall erweitert und verbessert werden. Neue Erkenntnisse im Verlauf einer Untersuchung erzeugen weitere Aufgaben. Die Mitglieder des Untersuchungsteams übernehmen im Werkzeug von Co3 Teilaufgaben und stellen die Ergebnisse den mitarbeitenden Experten zur Verfügung. Dadurch kann nicht nur sichergestellt werden, dass in hektischen Situationen die notwendigen Schritte effizient abgearbeitet werden. Es findet auch ständig eine zentrale Dokumentation und eine kontinuierliche Verbesserung des Prozesses statt.
Weitere Informationen:
 www.it-daily.net/award
Ansprechpartner:
Ulrich Parthier
it verlag GmbH
Michael-Kometer-Ring 5
85653 Aying
Telefon: +49-8104-649414
E-Mail: u.parthier@it-verlag.de
Über die it verlag für Informationstechnik GmbH:
Die it verlag für Informationstechnik GmbH publiziert das Magazin it management mit dem Supplements it security. Im Online-Bereich stehen mit der Website www.it-daily.net und diversen Newslettern wertvolle Informationsquellen für IT Professionals zur Verfügung. Mit Studien, eBooks und IT Research Notes unter dem Label IT Research sowie Konferenzen zu Themen des Print-Magazins rundet der Verlag sein Informationsangebot ab.
Tags
IT Sicherheit, IT Security, Web Security, Award, IT Security Award, Management Security, IRM, IAM, IDM, Identity
 Access Management, Authentifizierung, Hiscox, PASA, nmap, OpenVAS, Pallas, ForgeRock, Co3, Incident Response Prozess

Silvia Parthier
usp MarCom
Margarethenstr. 15
82054 Sauerlach
Telefon: +49-8104-666 362
E-Mail: parthier@uspmarcom.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=577273" width="1" height="1">

Pressekontakt

IT Verlag

85653 Aying

parthier@uspmarcom.de

Firmenkontakt

IT Verlag

85653 Aying

parthier@uspmarcom.de

Die it verlag für Informationstechnik GmbH publiziert das Magazin it management mit den Supplements it security. Im Online-Bereich stehen mit der Website www.it-daily.net und diversen Newslettern wertvolle Informationsquellen für IT Professionals zur Verfügung. Mit Studien unter dem Label IT Research und Konferenzen zu Themen des Print-Magazins rundet der Verlag sein Informationsangebot ab.