Fallstudie zum SafeNet Authentication Manager

Sicherer Remote-Zugriff für CANCOM-Mitarbeiter

Durch Übernahmen hat sich das Systemhaus CANCOM stark vergrößert. Um weiterhin einen sicheren Zugriff auf die Systeme gewährleisten zu können, benötigte das Unternehmen eine übergreifende Authentifizierungsplattform. Diese Fallstudie beleuchtet den neuen Remote-Access-Ansatz. lesen...

Mehr zum Thema:

- Starke Authentifizierung im Internet
- Linux-basierte Mittelstands-Appliance für sichere Authentisierung

NEUE FACHBEITRÄGE & INTERVIEWS

Das Problem der privaten Netzwerk-Nutzung im Unternehmen

Bandbreiten-Engpässe im WLAN vermeiden

Kaum ein Büro arbeitet ohne WLAN. Die geschäftliche Nutzung beispielsweise für Online-Konferenzen verschlingt dabei schon genug Bandbreite. Kommen dann noch persönliche Anwendungen hinzu, führt das zunehmenden zu Engpässen bei der Netzwerk-Bandbreite. lesen...

Ortung darf nicht der Mitarbeiter-Überwachung dienen

Standortdaten als Sicherheitsfaktor richtig nutzen

Das Orten mobiler Geräte ist mittlerweile gängige Praxis, sowohl bei der Netzwerk-Zugangskontrolle als auch bei Anti-Diebstahl-Lösungen. Dabei darf der Beschäftigtendatenschutz aber nicht aus dem Blick geraten, immerhin lässt sich die Geolokation zweckentfremden. lesen...

Interview mit Michael Helisch von HECOM Security Awareness Consulting

Security Awareness wird selten nachhaltig umgesetzt

Hinsichtlich der Security Awareness genügt es nicht, die IT-Anwender im Unternehmen einmal zu schulen. Das Wissen muss immer wieder aufgefrischt werden. Michael Helisch von HECOM Security Awareness Consulting hat sich mit SearchSecurity.de über das Thema nachhaltiges Sicherheitsbewusstsein unterhalten. lesen...

LIVE-WEBCAST AM 26.10.2012, 10:00 UHR

SIEM: Sicherheitsinformationen und Meldungen nicht nur verwalten, sondern begreifen

Notieren Sie sich gleich den Termin: **26.10.2012, 10.00 Uhr**

Das reine Verwalten und Analysieren von Logfiles ohne Zusammenhänge und Content zu kennen, ist nicht mehr zeitgemäss.

In diesem Webcast zeigen wir Ihnen, wie Sie mit Hilfe von *Sicherheitsinformations- und Ereignis-Management (SIEM)* **fundierte Sicherheitsinformationen gewinnen, Schlussfolgerungen ziehen** und so **schnell auf Vorfälle reagieren können.**

>> Melden Sie sich hier an!

Interview mit Michael Helisch von HECOM Security Awareness Consulting

Security Awareness wird selten nachhaltig umgesetzt

17.10.12 | Autor / Redakteur: Ralph Dombach / Stephen Augsten

Michael Helisch: „Der Mitarbeiter muss das Unternehmen schützen wollen."

Hinsichtlich der Security Awareness genügt es nicht, die IT-Anwender im Unternehmen einmal zu schulen. Das Wissen muss immer wieder aufgefrischt werden. Michael Helisch von HECOM Security Awareness Consulting hat sich mit SearchSecurity.de über das Thema nachhaltiges Sicherheitsbewusstsein unterhalten.

SearchSecurity.de: Offenbar genießt Security Awareness heute nicht mehr den Stellenwert, wie noch vor einigen Jahren. Was sind nach Ihrer Meinung die Ursachen, Budgeteinsparungen oder eine fehlende Wirksamkeit (ROSI) von Security Awareness?

Michael Helisch: Den Trend, dass Security Awareness Maßnahmen immer mehr unter den Tisch fallen, kann ich so nicht bestätigen. Im Gegenteil: der Druck zur nachhaltigen Sensibilisierung nimmt aus meiner Sicht zu – nicht zuletzt aufgrund der Tatsache, dass das rechtliche bzw. regulatorische Umfeld immer restriktiver wird.

Meiner Meinung nach ist allerdings festzustellen, dass Security Awareness nicht nachhaltig umgesetzt wird. Dies liegt unter anderem daran, dass viele Unternehmen das Thema methodisch falsch angehen. Security Awareness ist eben nicht nur ein Problem mangelnden Wissens und/oder mangelnder Begeisterung für das Thema Sicherheit.

FÜR SIE AUSGEWÄHLT

Schutzmaßnahmen - Schwachstellen - Kurve - Privatgeräte - Rodolf

Zu viele Mobilgeräte können das Netzwerk lahmlegen
BYOD = Bring Your Own Disaster?

Internet-Scan fördert Schwachstellen und öffentliche Passwörter zutage
HD Moore prangert Geräte- und System-Schwächen an

Bedrohungen
Threat-Report: Erstes Quartal 2012

IT-Security Management & Technology Conference 2012
Wie Hacker an sensible Daten kommen

Der CISO als Schnittstelle zwischen Mensch, Technik und Organisation
Neue Aufgaben und Verantwortungen für den CISO

BAUEN SIE EINE VERTEIDIGUNGSLINIE AUF!

Der Schutz Ihrer wertvollen und vertraulichen Informationen in Datenbanken ist eine **grundlegende Voraussetzung für die Integrität und Wahrung des Rufs** Ihres Unternehmens.

Wenn aus Awareness dauerhafte Compliance im eigentlichen Sinn des Wortes werden soll, ist an weiteren (methodischen) Stellschrauben zu drehen, vor allem in den Bereichen Organisation und Personal. Unternehmenskultur, Identifikation mit dem Unternehmen seien hier beispielsweise als Stichworte genannt. Im Security-Fachblatt Hakin9 habe ich mich insbesondere mit dem Thema Sicherheitskultur im Unternehmen beschäftigt.

Awareness wird immer ein „weiches Thema" bleiben, was insbesondere in puncto Erfolgsmessung gerne Anlass zu Diskussionen gibt. Auch damit wird man leben müssen.

SearchSecurity.de: Befindet sich der Mitarbeiter heute womöglich in einer Komfortzone, in der er erwartet, dass die Technik ihn vor allen Problemen zuverlässig schützt?

Michael Helisch: Aus Sicht des Anwenders wird Sicherheit, gerade im beruflichen Umfeld, einer ständigen Kosten-Nutzen-Abwägung unterzogen. Für das meist mit einem Mehraufwand verbundene, dauerhaft sicherheitskonforme Verhalten, braucht es aus seiner Perspektive eine geeignete (subjektive) Rechtfertigung.

Wissen um die Risiken und Folgen ist eine notwendige aber nicht ausreichende Rahmenbedingung. Der Mitarbeiter muss das Unternehmen schützen wollen – und zwar nicht nur, weil gerade ein wenig Marketing für Sicherheit gemacht wird. Er/sie wird dies auch ohne Marketing tun, wenn ihm/ihr das Unternehmen oder das Team in der er/sie arbeitet „lieb und teuer sind". Auch hier sind wir wieder beim Thema Identifikation mit dem eigenen Unternehmen als dem für den Erfolg der Awareness-Arbeit wichtigsten Faktor.

NEUESTE WHITEPAPER & WEBCASTS

Security-Update für den Channel
IT-SECURITY Online-Kongress 2012

Externer Datenschutz
Fünf Best Practices zum Schutz von Backup-Daten

Externe Datenträgerarchivierung
Schutz Ihrer Backups und schnelle Wiederherstellung im Katastrophenfall

MEISTGELESENE ARTIKEL

Microsoft Patchday Oktober 2012
Kritische Sicherheitslücke in Microsoft Office

Zwei-Faktor-Authentifizierung mit dem Smartphone
Zugriffsschutz im BYOD-Netzwerk

Zu viele Mobilgeräte können das Netzwerk lahmlegen
BYOD = Bring Your Own Disaster?

MEISTGELESENE ARTIKEL

Tipps und Maßnahmen zur Sensibilisierung für IT-Sicherheit
Security Awareness mit Humor und Personenbezug

Zu viele Mobilgeräte können das Netzwerk lahmlegen
BYOD = Bring Your Own Disaster?

Kontrolle über die Nutzung privater Mobilgeräte
BYOD erfordert ein Umdenken in der IT

NEUE WHITEPAPER UND WEBCASTS

Identity- und Access-Management
Passwort-Verwaltung für privilegierte Benutzerkonten

Tiefgreifender Schutz
Endpoint Security für Windows

Endpunkt-Schutz
Angriffsziel Endpoint

Application Control
Die Guten, die Bösen und die Unbekannten

Advanced Persistent Threats - wie schütze ich mich richtig?
Finden Sie Sicherheitslücken, bevor diese ausgenutzt werden

Interview mit Michael Helisch von HECOM Security Awareness Consulting

Security Awareness wird selten nachhaltig umgesetzt

17.10.12 | Autor / Redakteur: Ralph Dombach / Stephan Augsten

Security Awareness ist ein steter Prozess

SearchSecurity.de: Trotz technischer Maßnahmen, braucht es den Mitarbeiter, der z.B. wie eine Phishing-Attacke auf seine Identität erkennt. Auf welche Schwerpunkte sollte heutzutage Security Awareness besonderen Wert legen, um einen maximalen Nutzen zu bieten? Was können Sie empfehlen?

Michael Helisch: Erfolgreiche Sicherheitsmaßnahmen umsetzen heißt dafür zu sorgen, dass die drei wichtigsten Elemente der Sicherheitskette – ich nenne sie „die 3Ps der Sicherheit", nämlich Produkte, Personen und Prozesse – vernünftig ineinander greifen.

Dabei ist der Mensch das zentrale Kettenglied, da er die ihm zur Verfügung gestellten Sicherheitsprodukte adäquat bedienen muss und die definierten Sicherheitsprozesse mit Leben füllt. Ein Sicherheitsbewusstsein zu schaffen, um Compliance zu erreichen, ist ein ständiger und weit verzweigter (Veränderungs-)Prozess.

Wenn diese Einsicht bei allen Beteiligten vorhanden ist – insbesondere bei denen, die das Budget dafür zur Verfügung stellen – ist schon viel erreicht. Desweiteren gehören für mich die Punkte „Relevanz" der angesprochenen Themen für den Einzelnen und „Glaubwürdigkeit" im Sinne von aktivem Vorleben durch die Führungskraft zu den Top 3 der Erfolgsfaktoren.

FÜR SIE AUSGEWÄHLT
Zugriffsmanagement - Industriespionage
Das Sicherheitsrisiko durch Mitarbeiter einschätzen und minimieren
Verschiedene Arten von Insider Threats gefährden die IT-Sicherheit
Wolfgang Reibensples, CISO der EnBW, über Security Awareness
Das Management muss IT-Sicherheit vorleben
Best Practices bei der Sicherheitssensibilisierung
Security Awareness dank Erfahrung anderer
Kompendium zu Data Loss Prevention
Rundumschutz gegen Datenverlust
Versteckte Feinde und falsche Erwartungen
Woran Security Awareness im Unternehmen scheitert

BAUEN SIE EINE VERTEIDIGUNGSLINIE AUF!

Der Schutz Ihrer wertvollen und vertraulichen Informationen in Datenbanken ist eine

SearchSecurity.de: Wie sehen Sie die Zukunft von IT Sicherheit. Wird man auf Security Awareness irgendwann verzichten können oder muss man immer die menschlichen und technischen Aspekte berücksichtigen?

Michael Helisch: Um auf den ersten Teil der Frage zu antworten: Nein, sicher nicht, allein schon aufgrund der Tatsache, dass sich die Bedrohungsszenarien immer weiterentwickeln werden. Die entscheidende Frage ist: Was muss ich dafür an Aufwand betreiben?

Nachhaltig erfolgreich wird man dabei nur mit einen ganzheitlichen Ansatz, der deutlich über das Thema Sicherheit als solches hinaus geht und beispielsweise organisatorische wie auch personelle Themen integriert. Das macht es für den Awareness-Verantwortlichen nicht unbedingt leichter, es spiegelt aber die Komplexität wider, in der wir uns bei diesem Thema nun mal bewegen.

Michael Helisch ist Gründer und Inhaber von HECOM Security Awareness Consulting. Das Interview führte Ralph Dombach.

ERGÄNZENDES ZUM THEMA

Über Michael Helisch

Michael Helisch ist Gründer und Inhaber von HECOM Security Awareness Consulting und widmet sich bereits seit 2002 dem Thema Security Awareness. Neben zahlreichen Artikeln und Vorträgen hat Herr Helisch im Jahr 2009 zusammen mit Dietmar Pokoyski das erste Fachbuch im deutschsprachigen Raum zum Thema Security Awareness herausgegeben. Er ist Initator der D/A/CH-weiten Studienreihe „Security Awareness in der betrieblichen Praxis" und Dozent für Security Awareness an der FH Hagenberg.

Inhalt des Artikels: