Datum: 20.05.2016

Computerworld.ch

DT02

Computerworld
8032 Zürich
044/ 387 44 44
www.computerworld.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 8'303
Erscheinungsweise: 13x jährlich

Themen-Nr.: 663.132
Abo-Nr.: 3002182
Seite: 74
Fläche: 114'786 mm²

174.450

FIRMENFACHBEITRAG | Ergon

Foto: J. Wüst

Aktuelle Herausforderungen

IT-Security als Sicherheitsrisiko?!

IT-Sicherheitsmassnahmen müssen den Faktor Mensch berücksichtigen. Ein Interview mit dem IT-Security-Spezialisten Dr. Martin Burkhart über ein wichtiges Spannungsfeld. **Das Interview führte Annette Kielholz**

Datum: 20.05.2016

Computerworld.ch

DT02

Computerworld
8032 Zürich
044/ 387 44 44
www.computerworld.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 8'303
Erscheinungsweise: 13x jährlich

Themen-Nr.: 663.132
Abo-Nr.: 3002182
Seite: 74
Fläche: 114'786 mm²

174.450

Keine Digitalisierung ohne IT-Sicherheit – sie ist das Fundament aller geschäftskritischen Online-Transaktionen. Zu hohe Sicherheitsanforderungen können aber ebenfalls ein Risiko bedeuten –, weil sie den Faktor Mensch ausser Acht lassen. Ein Interview mit dem IT-Security-Spezialisten Dr. Martin Burkhart über aktuelle Herausforderungen im Spannungsfeld Sicherheit und Benutzerfreundlichkeit.

IT-Security war schon immer der Spielverderber, wenn es um Benutzerfreundlichkeit von IT-Anwendungen geht. Warum sind diese Themen so schwierig miteinander zu vereinen?

Das Spannungsfeld Sicherheit – Usability besteht, aber es ist weniger gegensätzlich, als man oft meint. Wir können den Spiess ja auch einmal umdrehen: Ohne IT-Security gäbe es nämlich gar kein Business im Internet. Stell mal eine Applikation ins Netz und kümmere dich nicht um die Sicherheit! Sie wäre innerhalb kürzester Zeit gehackt. Die beste Applikation nützt nichts, wenn sie nicht verfügbar ist.

Zudem kann gute Usability sogar die Security verbessern. Ein Beispiel, das wir alle kennen, sind Login-Systeme mit hohen Anforderungen an komplexe Passwörter, die dann auch noch monatlich geändert werden müssen. Damit erreicht man das Gegenteil dessen, was man will: Statt die Sicherheit zu erhöhen, schreiben die Benutzer ihre Passwörter einfach auf Post-ITs und kleben sie an den Bildschirm. Machen wir den Zugang für die Benutzer einfacher, zum Beispiel mit Single Sign-on, spielen sie eher mit und dadurch werden die Systeme sicherer.

Die Nutzerfreundlichkeit lässt aber auch heute noch zu wünschen übrig …

Ja, durch das Aufkommen von Smartphones und anderen Mobilgeräten hat die Komplexität zugenommen. Trotzdem will der User «Seamless Access», nämlich dass er seine Applikationen überall und sicher bedienen kann. Natürlich mit der gleichen Benutzerfreundlichkeit, die er sich von seinem Smartphone sowieso gewohnt ist. Die Erwartungshaltung ist – trotz der zunehmenden Komplexität – also klar gestiegen. Wir nehmen heute zwar über unsere Mobilgeräte die Geschäftsapplikationen mit ins Privatleben, sind aber nicht mehr bereit, eine Passwort-Streichliste aus der Schublade zu kramen.

Mehr technische Komplexität und gleichzeitig höhere Ansprüche der Kunden an Benutzerfreundlichkeit – auf Kosten der Security?

Als störend empfinden Benutzer vor allem interaktive Authentisierungsschritte, bei denen sie etwas tun oder eingeben müssen, um zu beweisen, dass sie derjenige sind, für den sie sich ausgeben. Als «Alternative» zu solchen interaktiven Schritten verfolgen wir heute einen risikobasierten Ansatz. Eine «smarte» Security-Software berücksichtigt Kontextinformationen während des Zugriffs einer Person auf eine Applikation.

Zum Beispiel wird die Tageszeit registriert, der Ort des Zugriffs, die Device-ID, Browser-Informationen … die Kombination dieser Informationen ermöglicht die Unterscheidung, ob ein Zugriff regulär, d. h. vom immer gleichen Arbeitsplatz, von zu Hause oder von einem Internet Café erfolgt. Dies sind keine harten Fakten, aber Indizien dafür, ob ein Betrug vorliegen könnte. Je nach Sicherheitsanforderungen an eine Applikation kann so ohne grösseren Aufwand genügend Sicherheit erreicht werden und die Zahl der interaktiven Authentisierungsschritte lässt sich reduzieren.

Wenn grundsätzlich eine höhere Sicherheit erforderlich ist, verbessert es die Akzeptanz beim Nutzer, wenn er als «Gegenleistung» dafür Single Sign-on erhält. Er muss dann vielleicht einmal einen SMS-Code abtippen, dafür erhält er für den Rest des Tages Zugriff auf alle relevanten Applikationen. Single Sign-on erlaubt meist auch die vereinfachte Verwaltung der Authentisierungsmittel durch den Benutzer selbst. Solche «User Self-services» entlasten auch den Help Desk, indem viele Routineanfragen wegfallen.

Unternehmen unterscheiden heute in einem Portal zwischen Bereichen mit verschiedenen Sicherheitsanforderungen. Der Hypothekenrechner einer Bank ist zum Beispiel nicht sicherheitskritisch, für einen personalisierten Börsenticker braucht es nur eine einfache Authentisierung, E-Banking muss jedoch stark authentisiert sein.

Dadurch wird die Konfiguration der Security-Anforderungen durch die Betreiber doch sehr komplex …

Ja, das ist nicht zu unterschätzen, und Fehlkonfigurationen durch Administratoren gehören mit zu den wichtigsten Einfallstoren für Cyberkriminelle. Ein Sicherheitsprodukt soll den Administrator so anleiten, dass er möglichst wenig Fehler machen kann und gewarnt wird, falls er sich aufs Glatteis begeben sollte. Wir investieren beim Konzipieren unserer Benutzeroberfläche besonders viel Zeit dafür, dem Administrator die wichtigsten Informationen auf einfache Weise zu präsentieren und Komplexität zu verstecken. Das geht so weit, dass wir sogar automatische Konfigurationsvorschläge generieren, basierend auf tatsächlichen Ereignissen. Der Administrator muss dann nur noch prüfen, welches der beste Vorschlag ist, und diesen freischalten. Dieses Feature, das «Policy Learning» genannt wird, stösst bei Kundengesprächen und bei unseren Schulungsteilnehmern auf sehr positive Resonanz.

Und was bringt die Zukunft?

Biometrie ist natürlich im Gespräch – dies aber schon seit vielen Jahren. Mit dem Fingerscanner und der Gesichts- und Iriserkennung über das Smartphone

Datum: 20.05.2016

Computerworld.ch

DT02

Computerworld
8032 Zürich
044/ 387 44 44
www.computerworld.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 8'303
Erscheinungsweise: 13x jährlich

Themen-Nr.: 663.132
Abo-Nr.: 3002182
Seite: 74
Fläche: 114'786 mm²

174.450

hat das Thema wieder an Aktualität gewonnen. Das Passwort als solches wird auch immer wieder infrage gestellt. Interessanterweise entstehen aber sogar bei diesem «Dinosaurier» der IT-Security neue Konzepte, die das Passwort wahrscheinlich auch in Zukunft überdauern lassen, wie das Beispiel unseres Forschungsprojekts mit IBM Research zeigt. ■

Dieser Beitrag wurde von der Firma Ergon zur Verfügung gestellt. Computerworld übernimmt für dessen Inhalt keine Verantwortung

Innovativer Passwortschutz

Airlock unterstützt IBM Research bei der Entwicklung optimal verteilter Passwort-Überprüfung

Airlock-Entwickler haben das IBM-Forschungszentrum in Zürich-Rüschlikon bei der Entwicklung eines hocheffizienten kryptographischen Protokolls zum Passwortschutz im Falle von Serverkompromittierung unterstützt. Die Passwort-Verifizierung wird dabei auf mehrere Server verteilt, so dass ein Angreifer sämtliche involvierten Server kompromittieren müsste, um Informationen über das Passwort zu erhalten. Das innovative Konzept ermöglicht es, einfache Passwörter auch bei mittelhohen Sicherheitsanforderungen und vielen Benutzern beizubehalten.

Der Interviewpartner

Dr. Martin Burkhart,
Produktmanager Airlock Suite,
Ergon Informatik AG

Nach einem Informatik-Studium an der ETH Zürich arbeitete Martin Burkhart zunächst als Softwareentwickler, bevor er an der ETH zur Anonymisierung von Netzwerkdaten und zu angewandter Kryptographie für kollaborative Sicherheitsprotokolle dissertierte.

Bei Ergon leitete Martin Burkhart seit 2012 IAM-Integrationsprojekte und ist seit 2013 für das Produktmanagement der Airlock Suite zuständig. Teil der Airlock Suite ist Airlock WAF, eine Web Application Firewall, die in der Schweiz ein de-facto Standard für den Schutz von Online-Banking ist. Sie wird international bei über 350 Unternehmen in Umgebungen mit hohen Sicherheitsanforderungen eingesetzt. Zusätzlich bietet die Airlock Suite mit Airlock IAM eine zentrale Authentifizierungsplattform mit Enterprise-Funktionen wie Single Sign-on oder User Self-services.

AIRLOCK by ergon