العدد الثالث
BLUEKAIZEN.ORG
يوليو/سبتمبر ٢٠١١

SecurityKaizen

your way to improve your security

العربية

مقابلة مع
جو سوليفان
مدير قسم أمن المعلومات
في موقع Facebook.com

فريق المجلة بمؤتمر
HITB
بأمستردام

مقابلة مع
آل برمان
المدير التنفيذي
لمؤسسة DRII الدولية

استمرار العمل
بالشرق الأوسط

هل أنت مستعد لكارثة؟

Security kaizen magazine

Media Sponsor

for

2011

Information Security Conferences

Conference	Date
Hacker Halted, Cairo	December 2010
TakeDowncon, Dallas	May 2011
HITB, Amsterdam	May 2011
MENA ISC, Jordan	September 2011
Cairo Security Camp	October 2011
HITB, Kualalumpur	October 2011
RSA, London	October 2011
Hacker Halted, Miami	October 2011

Register Now on www.bluekaizen.org and have the oppurtunity to **win free tickets** to our sponsored Conferences

Cairo Security CAMP 2011

The first annual Information Security Conference organized by an Arab Country

改善

BLUE KAIZEN

Connecting People & Improving Lives

Register Now!

http://www.bluekaizen.org/cscamp.html

Security kaizen magazine

كلمة العدد

لقد مرت ستة أشهر منذ إصدار عددنا الأول. وبمراجعة ما تم، يُمكنني أن أرى كيف تطورت المجلة طوال هذه الأشهر الستة، وكيف يتوسع المجتمع. فقد تم تنزيل العدد الأول ٩٠٠ مرة خلال سبعة أيام وتم تنزيل العدد الثاني ٢٧٠٠ مرة خلال ثلاثة أيام فقط. أنا أعلم بأنني قد اندهشت من عدد الأشخاص الذين كانوا على علم بمجلتنا في مؤتمر Cairo ICT؛ وقد كان من الرائع التحدُث شخصيًا إلى العديد من قُرائنا.

لقد كنا قادرين على دعم بعض المؤتمرات المرموقة إعلاميًا، مثل مؤتمر TakeDownCon Dallas ومؤتمر HITB Amsterdam. فإن الدعم يُساعدنا على تكثيف وجودنا ليس في مصر والشرق الأوسط فقط ولكن للوصول بمجلة سيكيوريتي كايزن (Security Kaizen) إلى خارج منطقة الشرق الأوسط وشمال أفريقيا والوصول إلى المزيد من القُراء في الولايات المتحدة الأمريكية وأوروبا. وقد أعطانا هذا أيضًا الفرصة لإجراء مقابلة مع جو سوليفان، مدير قسم الحماية في موقع Facebook.

فقد أصبح مُمثلي Mozilla، وGoogle، وMicrosoft، وAdobe الآن على علم بوجود مجلة بمجلة سيكيوريتي كايزن (Security Kaizen). وقد بدأنا في جذب الأنظار إلينا في مجتمع أمن المعلومات في كافة أنحاء العالم. ولذلك، يجب علي توجيه الشُكر لقُرائي وفريقي المُتخصص على هذا النجاح.

وسنحاول أن نجعل عددنا الثالث أكثر تميُزًا من خلال التركيز على موضوع واحد. فقد كانت الأحداث الأخيرة في مصر والشرق الأوسط درامية وغير طبيعية وقد عرضت تحديات غير مسبوقة للعمليات التُجارية وبخاصةً نُظم تكنولوجيا المعلومات. وأحد الدروس الرئيسية المُستفادة في هذا الموقف هو الحاجة لوجود خطط مرنة لاستمرارية العمل ومعالجة الكوارث، ولذا فإن هذا الموضوع هو محور العدد الجديد.

ولجعل العدد الثالث أكثر تميُزًا، أُعلن بمنتهى السعادة أن هذا هو أول عدد مطبوع من المجلة، وكما وعدنا وحيث أننا نحاول أن نتطور دائمًا، لقد كنا قادرين على تحسين كل عدد. فقد تم نشر العدد الأول في يناير ٢٠١١ وعلى الرغم من الظروف السائدة في مصر في هذه الفترة، إلا إننا كنا قادرين على نشر العدد الثاني في أبريل ٢٠١١ في إصدارين – باللغة الإنجليزية واللغة العربية. وأخيرًا عددنا الثالث المُميز على وشك أن يتم طباعته لتُتيح لكم، قُرائنا المُخلصين، مجالاً أكثر راحة أثناء القراءة.

معتز صلاح
رئيس التحرير

رئيس مجلس الادارة ورئيس التحرير
معتز صلاح

المحررين
محمود توفيق
معتز صلاح
عمر شيرين
فينوث سيفا سوبرامانيان
محمد محي الدين
محمد فرج

ترجمة
مي علاء الدين سعود
أسماء إبراهيم

تصميم موقع الإنترنت
مريم سامي

التصميم الجرافيكي
محمد فضلي

改善
BLUE KAIZEN

للإعلان بمجلة Security Kaizen
وموقع www.bluekaizen.org
Mail: Info@bluekiazen.org
Phone: 010 267 5570

Security Kaizen

يوليو/ سبتمبر ٢٠١١ . العدد الثالث

قصة حقيقية

أخبار وتقنيات

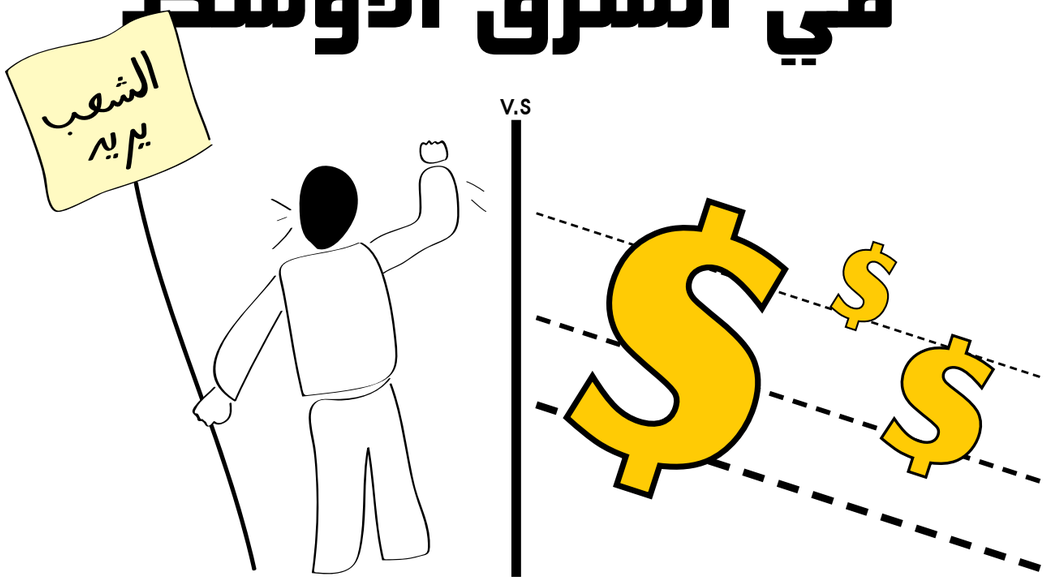
مقابلات

أفضل الطرق المتبعة

صورة الغلاف: محمد فضلي

استمرارية العمل

أثناء أحداث الاضطراب الأخيرة في الشرق الأوسط



في الأسابيع القليلة الماضية، كان الشرق الأوسط مسرحًا للتغييرات السياسية والاجتماعية السريعة غير المسبوقة والتي فاجأت أكثر الشركات نضجًا وتطورًا، وتركتهم تقريبًا في حالة من الشلل.

وحتى أكثر وكالات الاستخبارات السرية تعقيدًا ومعرفة لم تتوقع الثورات الاجتماعية واسعة النطاق التي تظهر في كافة أنحاء المنطقة.

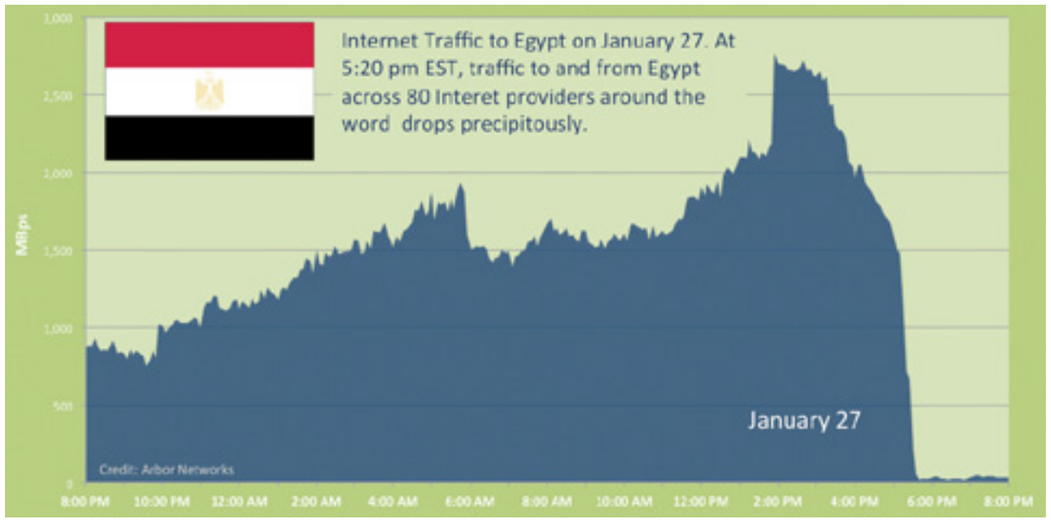
ويُعد تحليل استراتيجية استمرار العمل في مصر شيئًا من الجدير القيام به، لأن الدولة قد شهدت على الأرجح أول حدث يتم تسجيله لحكومة قامت بالفعل باستخدام «مفتاح إيقاف»[1] الإنترنت (kill switch)، بالإضافة إلى تأثير العواقب الناتجة عن هذا القرار. وإضافةً إلى ذلك، بما أن مصر تُعد ثاني أقوى بلد اقتصاديًا في القارة الأفريقية بعد جنوب أفريقيا، يوجد لديها الاقتصاد الأكثر تنوعًا في المنطقة وفقًا لمعايير الأمم المتحدة؛ ولذا، فأن التأثير على مختلف أنواع الأعمال يُعد واضح الرؤية وغير محدد لقطاع تجاري معين.

إلى أي مدى تأثر العمل بهذه الأحداث

وبعد أيام من استمرار المظاهرات المناهضة للحكومة والتي تم استخدام الإنترنت والشبكات الاجتماعية مثل Facebook وTwitter فيها كمنصات للتنظيم، قررت الإدارة السابقة قطع الإنترنت قبل منتصف ليل السابع والعشرون من يناير بدقائق على أمل أن تقوم بمنع المتظاهرين من استخدام أدوات الاتصال الخاصة بهم.

وبعد ذلك بدقائق، تم تأكيد عدم وجود اتصال إنترنت على الإطلاق عبر كافة أنحاء الدولة. وما كان يُعتبر يومًا مستحيلاً على المستوى التقني قد ثبت ليكون ممكنًا على المستوى التقني. وفي مثل هذه البلاد الاستبدادية، فإن العديد من البنية التحتية لوسائل الاتصال الافتراضية يكون تحت الملكية والسيطرة المباشرة للحكومة.

لقد رأينا مباشرةً التأثير المُفجع لقرار الحكومة المُندفع. تَصَور حرمان أحد البلدان أو أحد الأعمال الحديثة طوال الليل من رسائل البريد الإلكتروني، أو خدمات VoIP، أو التجارة الإلكترونية، أو إجراء الاجتماعات عبر الإنترنت، أو تصفح الويب، أو تشغيل الموقع الإلكتروني الخاص بإحدى الشركات، أو حتى البحث عن توفير الدعم عن بُعد عبر الإنترنت. ولقد استمر هذا الموقف غير المسبوق لمدة ٥ أيام عمل متتالية.



الشكل ١ – انقطاع الإنترنت في السابع والعشرين من يناير

التأثير المباشر

وكانت الشركات التي تعمل في مجال الاستعانة بمصادر خارجية في مجال صناعة تكنولوجيا المعلومات (IT) من بين أول الشركات التي تأثرت بالأحداث. لقد قدرت إحصائيات منظمة التعاون والتنمية الاقتصادية[٤] (OECD) الرسمية الخسارة المباشرة في الدخْل في تلك الأيام الخمس تراوحت ما بين ٩٠ مليون دولار إلى ١٢٠ مليون دولار والتي لا تتضمن فرص العمل الضائعة وخرق اتفاقيات مستوى الخدمة المُقدمة والدعاوي القضائية المحتملة.

ويُعد القطاع المصرفي مثالاً آخر من الهيئات التي تأثرت بالأحداث في مصر. فقد أعلنت العديد من البنوك المحلية والدولية أن الخدمات الرئيسية مثل تحويل الأموال والخدمات المصرفية عبر الإنترنت غير متاحة أو لا يُمكن الاعتماد عليها. ومع إيقاف تشغيل شبكة الصراف الآلي (أي تي أم – ATM) المحلية وتخريب ماكينات الصراف الآلي (أي تي أم – ATM)، فقد لجأ الملايين من عملاء البنوك إلى الوقوف في صفوف طويلة أمام فروع البنوك المحلية الخاصة بهم. ولسوء الحظ، لا يوجد حتى الآن أية دراسات رسمية حول التأثيرات المترتبة على النقص في السيولة المادية في الأعمال الصغيرة.

كيفية تنفيذ خطط استمرارية العمل

لقد ظهر عدم تأثُّر عدد قليل جدًا من الشركات وتكيفها مع الوضع. ولقد نجت بعض الشركات نتيجة لتنفيذ خطط ثابتة لاستمرارية العمل (BCPs) ومع ذلك فقد استمرت الشركات الأخرى في العمل فقط بسبب الحظ.

يُعد أحد مُشغلي خدمة الهاتف المحمول مثالاً جيدًا للشركة التي نجت من الاضطرابات بفضل خطة استمرارية العمل الثابتة والشاملة.

وفي السابع والعشرون من يناير، لقد تم إطلاق خطة استمرارية العمل عندما قامت الحكومة بقطع الإنترنت. عندئذٍ اجتمع فريق إدارة الأزمات (CMT) وقام بتنشيط خطة معالجة الكوارث (DRP) لإيقاف تشغيل خدمات تكنولوجيا المعلومات (IT) المحلية بأمان وقام الفريق بالتركيز على تأمين الأصول المادية، ومراكز معالجة البيانات، وأبراج الاتصالات الخلوية الرئيسية، ومحطات توليد الطاقة، من التخريب وربما من النهب أيضًا نظرًا لأعمال الشغب والاشتباكات الموجودة في الشوارع.

في البداية، لقد أُمطرت مراكز خدمة العملاء بالعديد من المكالمات للشكوى من صعوبة استخدام خدمات الاتصال مثل خدمة الإنترنت عبر الهاتف المحمول، وخدمات البلاك بيري (Blackberry)، وحتى المكالمات الدولية. وعلى الرغم من محاولة مُمثلي خدمة العملاء شرح الموقف للمُتصلين، فقد أدركوا لاحقًا أن المشكلة كانت قومية.

وفي التاسع والعشرون من يناير، أعلنت الحكومة حالة من الطوارئ القومية وتم فرض حظر التجول. علاوةً على ذلك، تلقى جميع مُشغلي خدمة الهاتف المحمول في الدولة أوامر من الحكومة بإيقاف تشغيل اتصالات الهاتف المحمول بما في ذلك خدمات الرسائل القصيرة (SMS) كمحاولة أخيرة لتعطيل اتصالات المتظاهرين.

وبسبب وجود بند في اتفاقيات ترخيص الهاتف المحمول التنظيمية والتي تم توقيعها مع جميع مُشغلي خدمات الهاتف المحمول، لذا كان يجب على الشركات الامتثال لهذا القرار. ولقد أثبت هذا القرار تأثيره المُكلف والسلبي بشكل واضح على صورة الشركات بسبب تلقي الشعب هذا التصرف من مُشغلي وسائل الاتصالات على أنه إشارة على مساعدة نظام الحكم السابق والانحياز ضد العملاء.

وفي الأسابيع القليلة الماضية، قام العديد من العملاء ونشطاء الحقوق المدنية بتجميع الشعب حولهم والمنادة بيوم وطني لمقاطعة خدمات الهاتف المحمولة لمدة ٣٠ دقيقة بالإضافة إلى رفع العشرات من الدعاوي القضائية ضد مُشغلي الخدمة.

وفي هذه المرحلة، قامت فرق إدارة الأزمات بإصدار الأوامر بإيقاف تشغيل مراكز خدمة العملاء والخطوط الأرضية وتم تنشيط شجرة المكالمات الداخلية وأمرت جميع الموظفون بالبقاء في المنزل حتى إشعار آخر.

وبعد تلقي تأكيد إجلاء المقار الرئيسية ومكاتب الفروع في أنحاء الدولة وقفلها، فقد بدأ فريق إدارة الأزمات (CMT) خطة الاتصالات أثناء الأزمات (CCP). ومن المتطلبات الرئيسية لخطة الاتصالات أثناء الأزمات هي توصيل رسائل تحديث الحالة المناسبة إلى وسائل الإعلام الدولية والأسواق المالية الأجنبية التي تم إدراج الشركة فيها.

وعلى جانب تكنولوجيا المعلومات (IT) فيما يخُص الاضطراب، فقد تم تصميم خطة معالجة الكوارث الخاصة بهذه الشركة لتُخفف من مخاطر الخسارة التامة في مجال الاتصالات من خلال تطوير نسخة طبق الأصل من خدمات الويب الخاصة بهذه الشركة المُستضافة في أوروبا وكذلك من خلال التوقيع مع مُزود شهير للخدمات التي يتم إدارتها اعتمادًا على الشبكة ليقوم بإدارة تواجد رسائل البريد الإلكتروني الخاصة بالشركة وحمايتها لـ ٥٠٠٠ مستخدم في الشبكة. ويوجد لدى هذه الخدمة التي يتم إدارتها من قِبل المزود بندًا يتيح لهم حفظ مسودات لرسائل البريد الإلكتروني التي لم يتم تسليمها حتى سبعة أيام «في الشبكة». وقد عاد الإنترنت بمجرد قيام الرئيس السابق وإدارته بإعلان استقالتهم وأُغمرت صناديق البريد الإلكتروني الخاصة بالموظفين برسائل الأسبوع المُنقضي، وبالتأكيد يعد هذا الموقف أفضل من الحصول على صندوق بريد خالي وحفنة من العملاء الغاضبين.

ومن جهة أخرى، فقد أثبتت المؤسسات مثل البورصة المصرية (egyptSE.com) وبعض البنوك التي بدت متصلة بالإنترنت ويُمكن الوصول إليهم أثناء انقطاع الإنترنت إنهم كانوا متصلين عبر مُزود خدمة إنترنت موحَّد وصغير بعض الشيء فيما يتعلق بنصيب السوق (٨٪ تقريبًا) ويُسمى مجموعة نور (Noor Group)[٥]. وكان من الواضح أن مجموعة نور هي الإستثناء الوحيد في هذا الوقت. ومن غير الواضح ما إذا كان مُزود خدمة الإنترنت (ISP) قد صمد أمام قرار الحكومة السابقة من قبيل المصادفة أو بسبب قائمة العملاء الاستراتيجية بما في ذلك العملاء الشبيهون بالبورصة.

بناءًا على المعلومات المتاحة، فإن ما يقرُب من ٨٠٪ من الأعمال لم تُدرِج سيناريو انقطاع الإنترنت القومي كاحتمال قوي وتبعًا لذلك لم يكونوا مستعدين لمواجهة هذا الموقف.

وكانت نسبة الـ ٢٠٪ المُتبقية من الشركات إما مُستعدة جيدًا بطرق بديلة ومتعددة من وسائل الاتصال الدولية مثل اتصال الأقمار الصناعية «فيسات» ("VSAT") أو الشركات التي لا تعتمد على الإنترنت على وجه الحصر في عملها.

من الذي صمد أمام هذا القرار؟

وحيث إن أكثر وكالات الاستخبارات السرية تقدُمًا في العالم مثل وكالة الاستخبارات المركزية الأمريكية (CIA) لم تتوقع هذه الثورة «بالقدر الذي نعرفه»، فقد وصفت هيلاري كلينتون - وزيرة الخارجية الأمريكية – الحكومة المصرية بأنها «مستقرة»[٢] حتى بعد ثلاثة أيام من الأحداث الدرامية. ومن المثير للانتباه، لم تتنبأ أيًا من طرق تقييم المخاطر التقليدية المتاحة أو المعمول بها في

معظم الشركات في مصر بمثل هذا الخطر من الإصلاح السياسي البالغ والثورة الاجتماعية.

ومن المُلفت للانتباه أن هذا العرض يُعد عرضًا عالميًا لحكومة تقوم باستخدام «مفتاح إيقاف» الإنترنت مقرونًا بانقطاع اتصالات الهاتف المحمول في كافة أنحاء البلد. وقد أخذ ذلك الجميع على حين غرة.

كان يجب على خبراء المخاطر في الشركة التعلُّم من تجربتهم السابقة في عام ٢٠٠٨ عندما حدث اضطراب بالغ في خدمات الإنترنت الذي سبّبهُ قطع كبل الإنترنت الموجود تحت سطح البحر[٣].

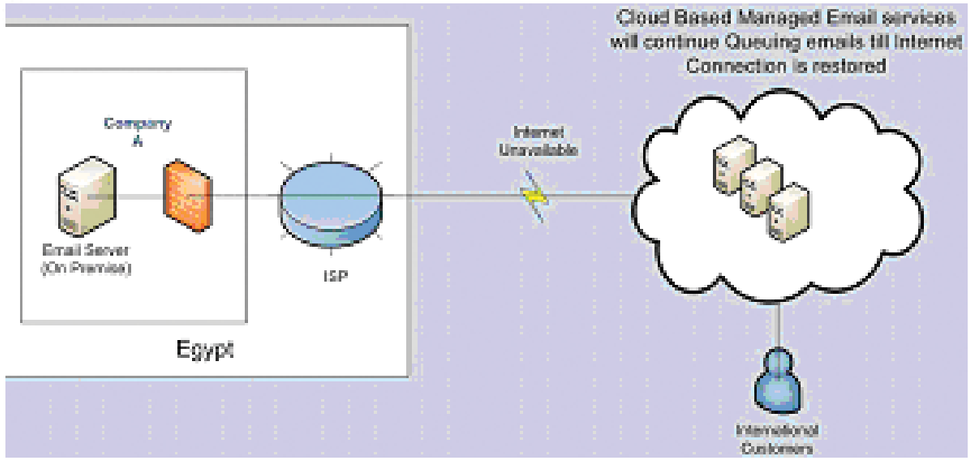
والفشل في التنبؤ بمثل هذه الحادثة البالغة وتضمنها في مصفوفة المخاطر الخاصة بالشركة هو أمر غير مسموحٍ به.

وربما كانت الشركات الوحيدة التي واصلت العمل أثناء أحداث شهر يناير ٢٠١١ «وحتى إعلان حالة الطوارئ وحظر التجول العام» هي الشركات التي لديها ممارسات شديدة ونشِطة وديناميكية لتقييم المخاطر والتي تعلمت من أحداث عام ٢٠٠٨ وقامت باستخدام هذه الدروس وتحويلها إلى سيناريوهات كوارث قابلة للنمو. وفي ظاهر الأمر، هذا ليس سهلاً كما يبدو وبما أن معظم الشركات واجهت مشاكل خاصةً عندما يتعلق الأمر بتطوير نظام التغذية العكسية لضمان قيام المؤسسة بمواصلة المراجعة، والدمج، والتعلُّم من التجربة والتعامل مع التهديدات الناشئة والجديدة والتي كانت مُحالة ولم يسبق لها مثيل منذ عامين.

والملاحظة الأساسية هي أن الشركات التي قامت باستخدام حوسبة الشبكة هي التي كانت سهلة التكيُف وقادرة على العمل بشكل ملحوظ أثناء الاضطرابات بسبب المرونة والتواجد المُقدمان بواسطة بنية حوسبة الشبكة.

التواجد المعتمد على الشبكة

تتيح بنية التواجد العالي المعتمدة على الشبكة للشركات الاستعانة بمصادر خارجية لإدارة النظم الدقيقة الخاصة بهم وصيانتها مثل البريد الإلكتروني على سبيل المثال، ونقل أرشفة البريد الإلكتروني ووظائف التواجد العالية إلى الشبكة. كما هو موضح في الرسم التوضيحي الموجود أدناه (الشكل ٢)



الشكل ٢ – نظام البريد الإليكتروني الذي يتم إدارته اعتمادا على الشبكة

يقوم النظام بتخزين رسائل البريد الإلكتروني الخارجية بشكل آمن وسليم في الشبكة. ولذلك، إذا كان مركز خدمة رسائل البريد الإلكتروني الخاص بشركتك غير متاح كما هو الحال في حالة انقطاع الإنترنت، فإن خدمة البريد الإلكتروني التي يتم إدارتها اعتمادًا على الشبكة ستقوم بمواصلة استلام رسائل البريد الإلكتروني المُرسلة إلى شركتك بالنيابة عن الشركة (بينما أنت في الواقع غير متصل بالإنترنت)، وكل هذا واضح بالنسبة للمُرسل، على سبيل المثال مثل العملاء الدوليين. وهذا يضمن بقاء صورة شركتك سليمة مع عدم فقدان أي فرص للعمل.

نقاط ضعف الممارسات التقليدية لاستمرارية العمل (BC)/معالجة الكوارث (DR)

لقد وجدت العديد من الأعمال الصغيرة إلى المتوسطة الحجم التي يوجد لديها خطط استمرارية العمل (BC) وخطط معالجة الكوارث (DR) تقليدية أن الخطط الخاصة بهم يوجد بها العديد من نقاط الضعف في التعامل مع هذا الموقف على وجه الخصوص بسبب الاعتماد على التكنولوجيا الحديثة. وبعكس ما هو متوقع، فإن العديد من الشركات لم تكن قادرة على تنشيط شجرة المكالمات الخاصة بها بسبب عدم إتاحة الهواتف المحمولة والرسائل القصيرة وكان نشر رسالة إلى مكاتب الفرع عبر الدولة يُعد تقريبًا مستحيلاً.

وحتى الشركات التي يوجد لديها مواقع معالجة كوارث غالية (التي تقع على بُعد ١٠٠ ميل) كان يوجد لديها مشاكل في تنشيط خطة معالجة الكوارث (DRP) بسبب الخسارة الكاملة وطويلة المدى في مجال الاتصالات وعدم القدرة على البحث عن الدعم التقني من الشركاء والبائعين، بما في ذلك شركات صناعة الرقائق الزرقاء.

لقد أكدت الأحداث الأخيرة كيف أن الأعمال الحديثة تعتمد بالفعل على التكنولوجيا وخاصةً الإنترنت بالإضافة إلى التذكير المؤسف بأننا نُعد هذه التكنولوجيا الحديثة امرًا مفترضًا ومُسَلَم به.

المراجع:

١ مفتاح إيقاف الإنترنت (Internet Kill Switch)
(http://www.infowars.com/egypts-internet-kill-switch-coming-to-america/)

٢ تعليق هيلاري كلينتون على أحداث يوم الثامن والعشرون (Hillary Clinton comment on the events on the 28th)
(http://af.reuters.com/article/topNews/idAFJOE70O0KF20110125)

٣ انقطاع كبل الإنترنت تحت سطح البحر (Undersea cable cut)
(http://news.bbc.co.uk/2/hi/7792688.stm)

٤ إحصائيات منظمة التعاون والتنمية الاقتصادية حول إيقاف تشغيل الإنترنت (OECD statistics on cost of internet shut down)
(http://www.pcmag.com/article20,2817,2379324,00/.asp)

٥ لماذا كانت مجموعة نور متصلة بالإنترنت؟ (Why is Noor Online?)
(http://www.huffingtonpost.com/201131/01//egypt-internet-noor-group_n_816214.html)

الأشكال:

١ مفتاح إيقاف الإنترنت (Internet Kill Switch) – المصدر: شبكات (Arbor Networks Arbor)

٢ البريد الإليكتروني المُدار المعتمد على الشبكة

زيارة إلى مؤتمر HITB

بقلم: معتز صلاح

نبدأ مقالنا بمقدمة ونبذة بسيطة عن مؤتمر **HACK IN THE BOX (HITB)** لمن لم يسمع عنه من قبل. تُعد منظمة **HITB** من المنظمات المعروفة في مجال أمن تكنولوجيا المعلومات. وتقوم المنظمة بإجراء ثلاث مؤتمرات رئيسية سنويًا، في ماليزيا، وهولندا، وسيُقام المؤتمر هذا العام في الهند بدلاً من دولة الإمارات العربية المتحدة.

وكجزء من مهمتنا المتواصلة لتقديم آخر أحداث أمن المعلومات إلى قُرائنا، فقد شاركت مجلة سيكيوريتي كايزن (Security Kaizen) كراعي إعلامي في مؤتمر HITB المُقام بأمستردام. وقد حضر فريقنا المؤتمر الذي استمر لمدة يومان. وقد حصلوا أيضًا على فرصة لمقابلة المتخصصين ونقل الصورة كاملة على قدر الإمكان لأولئك الذين لم يمكنوا من الحضور.

وقد كانت تجربة حضور مؤتمر دولي كهذا جيدة حيث يتجمع العديد من متخصصي أمن المعلومات حول العالم لغرض واحد فقط، ألا وهو مشاركة معرفتهم وخبراتهم.

ومن حيث التنظيم، فإن أمستردام تُعد اختيارًا رائعًا كموقع ليُقام المؤتمر فيه. فأمستردام تُعتبر واحدة من أكثر الأماكن شهرة في أوروبا، كما إنها أحد هذه الأماكن التي تُقدم مجموعة من الأنشطة السياحية المتنوعة لتقوم بها في أوقات الفراغ.

وقد كان اختيار الفندق الذي تمت إقامة المؤتمر به اختيارًا دقيقًا جدًا، حيث يقع الفندق في قلب العاصمة أمستردام ويطل على ميدان دام (Dam Square) الشهير جدًا، ولذلك كان من الصعب أن تضل طريقك في محاولة العثور على الفندق، وكونه يقع في منتصف ميدان دام (Dam Square) يسمح لجميع الحاضرين بالقيام بجولات قصيرة بعد الدورات.

وقد بدأ المؤتمر بالخطبة التي ألقاها جو سوليفان، مدير قسم أمن المعلومات في موقع الـ Facebook (Facebook.com)). فقد قام بالتركيز على تهديدات الحماية التي يتعامل معها موقع الـ Facebook كل يوم. وقد وصف أيضًا كيف قام موظفي موقع الـ Facebook مؤخرًا بإطلاق عدد من ميزات أمن المعلومات الفريدة التي تعزز التخطيط الاجتماعي. وقد ذكر أيضًا حظر الوصول إلى موقع الـ Facebook خلال الأحداث الأخيرة في تونس، ومصر، وسوريا. أنا لن أتطرق إلى تفاصيل خطبته هنا، حيث يُمكنك إلقاء نظرة على المقابلة الحصرية التي أجراها جو سوليفان مع مجلة سيكيوريتي كايزن (Security Kaizen) حول هذا الموضوع.

وقد انقسم المؤتمر بعد هذه الدورة إلى ثلاثة مسارات، كل مسار يُغطي موضوع مختلف، ويجب عليك اختيار مسارًا واحدًا من الثلاثة. ولأكون صادقًا، أنا لم أُحب هذه الفكرة، لأنني رغبت بحضور دورات مختلفة تعارض توقيتها مع توقيت الدورات الأخرى. أيضًا لم يكن عدد الحاضرين كبيرًا. فبعد توزيع الحاضرين على ثلاث غرف، كان من الممكن أن تجد أن عدد الحاضرين في بعض الدورات لا يتعدى ١٠ إلى ١٥ شخصًا؛ وهذا لم يكن مظهرًا جيدًا بالطبع.

ومن أمثلة العروض التقديمية الجيدة في المؤتمر هو العرض التقديمي الخاص بـ«تحليل ملفات PDF الضارة»؛ وقد قام ديدر ستيفين (مستشار أمن المعلومات) بتقديم هذه الدورة. وقد استمرت الدورة لمدة ساعتين في المعمل،

وكانت مليئة بالعديد من الأنشطة العملية لتوضيح كيفية تحليل ملفات PDF الضارة بواسطة استخدام عملية الخطوة-بخطوة بدءًا من تدريب رقم (١) الذي كان يدور حول كيفية إخراج رسالة مخفية في ملف PDF وحتى تدريب رقم (١٢) الذي أظهر كيفية إخراج الرمز الضار من الملف. فقد قام المُدرب بتوفير أقراص رقمية (DVD) تحتوي على آلة افتراضية (VM machine)، والأدوات، والوثائق، والتدريبات لجميع الحاضرين، وقد كانت هذه المواد أكثر من المواد التي قاموا باستخدامها في المعمل، حتى يتمكنوا من القيام باختبارها في المنزل. ولا بد لي من الاعتراف بأن هذه الدورة كانت الأكثر إفادة بالنسبة لي في مؤتمر HITB.

وقد بدأ اليوم الثاني من المؤتمر بمداولة حول «استغلال نقاط ضعف الاقتصاد» ويضم ممثلين كلٍ من Google، وMicrosoft، وMozilla، وAdobe، وBlackberry. لقد كانت المداولة حيوية جدًا بين المتحدثين والحضور، كما لم يستطع بعض الحاضرين فهم لما لا يقوم الوكلاء بمكافأة الباحثين المستقلين ممن يقوموا باكتشاف نقاط الضعف في منتجاتهم، وخصوصًا مع وجود السوق السوداء لنقاط الضعف البديل والأكثر ربحية. وفي ظل غياب نظام إيجابي للمكافآت، فإنه من الصعب إلقاء اللوم على باحثي نقاط الضعف في توجههم إلى السوق السوداء والحصول على مقابل أكبر بصورة ملحوظة مما يُمكن الحصول عليه من برامج المسابقات مثل تلك التي يُقدمها موقع Google. لقد كانت المداولة مرحة وممتعة وقد أظهرت بوضوح حقيقة وجود سوق سوداء لنقاط الضعف فعليًا، والشيء الأكثر أهمية هو أنه مُربح بالفعل.

وفي النهاية، لقد كان مؤتمر HITB الذي أُقيم في أمستردام تجربة جيدة، كما كان يُمكنك الشعور بالدفء والمحبة والمجهود الذي بذله جميع أفراد طاقم HITB. كما أود أن أتوجه بالشُكر لـ ديلون (مؤسس HITB) على مجهوداته وعلى أفراد الطاقم الرائع الذي قام بتكوينه. وما لا يعلمه معظم الأشخاص هو أن أفراد طاقم HITB جميعًا من المتطوعين؛ وهم مدفوعين بمبادئ نشر المعلومات والمعرفة.

مع تمانيتنا لكم بكل التوفيق في حضور مؤتمر HITB المُقبل في ماليزيا!

للحصول على المواد الخاصة بالمؤتمر، يُرجى زيارة الموقع:

http://conference.hitb.org/hitbsecconf2011ams/materials/

ArabBSD
التطور الجديد
لمطوري أنظمة التشغيل العرب

بقلم: محمد فرج

يُعد ArabBSD مشروعًا يهدف إلى زيادة الوعي بتطوير ومساعدة مُطوري أنظمة التشغيل العرب في مجال BSD بدءًا من تحليل البنية التحتية لأنظمة التشغيل FreeBSD، وصياغة المُخطط الصندوقي (block diagram) ومُنادة مجموعات الأبحاث في كل مسار.

لقد أصبحت الحاجة للعمل في مسارات مستقرة رغبة العديد من المُبرمجين. فإن فهم برمجة أنظمة التشغيل يلفت انتباه المُبرمجين ويدفعهم إلى تصنيفه إلى حدٍ كبير.

وتطلب برمجة أنظمة التشغيل (OS) أيضًا إلى الذكاء لتطبيق القيود من البرامج الموجودة على الأجهزة وتوفير التوافق بين مختلف الوحدات الطرفية والمعالج، وهذا يخلق نوعًا من المنافسة لمن يُحب التحديات. وبوضوح أكثر، يعمل نظام التشغيل كطبقة وسيطة بين البرامج والأجهزة. وإحدَاث أية تغييرات في واجهات برمجة التطبيقات Kernel API سيؤثر على تطبيق الطبقة الأعلى لتكون غير قابلة للتشغيل أو لتعمل بشكل غير صحيح. ومن نظام التشغيل، يُمكنك اختيار أفضل بيئة تُناسب الرمز الخاص بك، أي الشبكة، أو أنظمة الملفات، أو الأنظمة المُضمّنة، أو الحماية، أو قاعدة البيانات، أو برمجة الشبكة.

يتم إنجاز العمل في ArabBSD في اتجاهين مُتوازيين. الاتجاه الأول هو ترجمة توثيق نظام تشغيل FreeBSD وبرامجه التعليمية إلى اللغة العربية بجانب ترجمة

موقع الويب الخاص بالمشروع. ويُقدم الاتجاه الثاني تدريب صيفي مجاني لبدء العمل في تطوير نظام تشغيل FreeBSD. ولكن لماذا تم اختيار أنظمة BSD؟!

تُعد توزيعة برامج بيركلي (BSD، وتُسمى أحيانًا ببيركلى يونكس [Berkeley Unix]) من مشتقات نظام تشغيل UNIX التي تم توزيعها بواسطة جامعة كاليفورنيا، بيركلي، بدايةً من السبعينات. ويُستخدم هذا الاسم بالإجماع للإصدارات الحديثة من هذه التوزيعات.

مُدمج)، وقد شهدت إصدارات المصدر المفتوح المُعدلة لرمز المصدر (وتكون غالبًا مُشتقة من إصدار 4.4BSD-Lite) في السنوات الأخيرة زيادة في الاستخدام والتطوير. ويُصنف نظام التشغيل FreeBSD كأحد أكثر أنظمة التشغيل المُؤَمنة والتي يُمكن الاعتماد عليها وفقًا للموقع http://news.netcraft.com. وأيضًا يقودنا تواجد أعضاء فريق FreeBSD الرئيسي وتعاونهم الكامل إلى اعتبار ذلك كبيئة التطوير. ولم أنسى أن أذكُر أن مراكز خدمة CISCO وYahoo هي «آلالات FreeBSD».

لقد تم الربط بين أنظمة BSD وإصدارات أنظمة تشغيل UNIX المتاحة على نطاق واسع لأنظمة فئة مكاتب العمل. ويُمكن إسناد هذا إلى السهولة التي يُمكن من خلالها ترخيص هذه الأنظمة والشهرة التي اكتسبتها بين شركات التكنولوجيا في الثمانينات. وقد أُكتسبت هذه الشهرة عادةً من استخدام الأنظمة المُشابهة – وخصوصًا أنظمة تشغيل DEC›s Ultrix وSun's SunOS – أثناء مرحلة تعليمهم. وبينما تم استبدال أنظمة BSD ذاتها إلى حدٍ كبير بأنظمة System V Release 4 وOSF/1 في التسعينات (فإن كلاً منهما يحتوي على رمز BSD

وفيما يتعلق بالتقدم الحالي، فقد تم إنجاز بعض العمل في مجال ترجمة البرامج التعليمية ونحن نواظب على العمل بجِد للوصول إلى الأفضل. وأخيرًا، يُمكن لأي شخص مُهتم بأنظمة التشغيل وبأخبارها الانضمام إلينا على موقع الويب https://sites.google.com/site/arabbsd/ ، أو مجموعتنا على موقع Facebook، أو قائمة Google البريدية الخاصة بنا. وسيقوم الأعضاء بمتابعة مشاكل أنظمة التشغيل لكلا جانبي الإدارة والتطوير بما في ذلك التخصص في كافة أنواع البرمجة.

أحداث القرصنة الأخيرة في مصر والشرق الأوسط

في هذا المقال, لقد قمنا بجمع بعض هجمات القرصنة الإلكترونية التي حدثت للحكومات والبنوك ووسائل الإعلام في مصر والشرق الأوسط خلال الشهور الأخيرة. ونود أن نتوجه بالشكر لـ «أسامة كمال» علي مجهوداته لمساعدتنا في تجميع هذه المعلومات.

محتوي هذا المقال لا يعبر عن رأي المجلة في الأحداث.
ببساطة، نحن نقوم بعرض حوادث مسجلة.

قطاع وسائل الإعلام:

يوم الأحد ٥ يونيو ٢٠١١، تم اختراق موقع الويب الخاص بجريدة أخبار اليوم علي الإنترنت

لقد تم اختراق موقع الويب الخاص بجريدة أخبار اليوم علي الانترنت بسبب رسم كاريكاتوري رسمه مصطفي حسين وأحمد رجب عن الحركة السلفية في مصر. وقد ادعى الشخص الذي قام باختراق الموقع أنه ليس سلفي لكنه مسلم ولا يقبل أن يسخرأحد من إخوته المسلمين ومن المسلمات اللاتي يرتدين النقاب. وقال أيضًا أنه لا أحد يجرؤ أن يسخر من المسيحيين بتلك الطريقة، كما تعجب من دعوة الصحيفة إلي الحوار والتسامح وحرية التعبير وهم يسخرون من المسلمين. وقد أبدى غضبه وتعجُبه من السخرية المسلمات اللاتي يرتدين النقاب على الرغم من أن هذه حرية شخصية.

الجمعة ٤ فبراير ٢٠١١ تعرض موقع الويب الخاص بقناة الجزيرة للاختراق

لقد كانت قناة الجزيرة ووكالات أنباء مختلفة تبذل جهدًا كبيرًا في الأشهر الأخيرة لتغطية أحداث الثورات المصرية والتونسية. ومع ذلك، فإن بعض الأشخاص لم تعجبهم طريقة قناة الجزيرة في تغطية تلك الأحداث إلى حد محاولة حجب بثها علي القمر الصناعي «نايل سات». ولذلك، لقد قام قرصان مجهول الهوية باختراق موقع الويب الخاص بقناة الجزيرة (Aljazeera.net) وكتب هذه الرسالة «معًا لإسقاط مصر».

الأربعاء في ٢٠ مارس ٢٠١١ تم اختراق موقع الويب الخاص بقناة اون تي في (ON TV) التليفزيونية

لقد اخترق موقع الويب الخاص بقناة اون تي في (ON TV) التليفزيونية شخصًا مجهول الهوية يُدعى (A-Alexand). وقد ترك رسالة علي الموقع تقول: « زواج السلطة بالمال يُولد الفساد، لا لاستغلال المال لتوجيه السلطة أو السياسة... نعم لمصر خالية من الفساد». كما أرسل تحذيرًا لنجيب ساويرس، مالك القناة، يطالبه بوقف شن حملات هجومية ضد الإسلام.

This page was h@cked

القطاع الحكومي:

في يونيو ٢٠١١، تم نشر كلمات السر الخاصة بمواقع الويب الحكومية في البحرين ومصر والأردن والمغرب على الإنترنت

لقد تم اختراق البريد الإلكتروني الخاص بعدد من مسئولي وكالات الحكومة المصرية بما في ذلك وزارة الاتصالات وتكنولوجيا المعلومات, والجهاز القومي لتنظيم الاتصالات (NTRA), ومركز المعلومات ودعم اتخاذ القرارات لمجلس الوزراء (IDSC). وقد قامت مجلة سيكيوريتي كايزن (Security Kaizen) بالإبلاغ عن هذه الحادثة لمركز الاستجابة لطوارئ الشبكات ونظم المعلومات (EGCERT) الذين شرعوا في التحقيق في الحادث. وقد حدث الأمر ذاته في البحرين والأردن والمغرب.

يونيو ٢٠١١، اختراق مواقع الويب الرسمية للحكومة البحرينية

قام القراصنة بشن مجموعة من الهجمات علي مواقع الويب الحكومية بعد قرار المجلس العالمي لرياضة السيارات التابع للاتحاد الدولي للسيارات المتضمن إعادة جدولة سباق جائزة البحرين الكبرى لطيران الخليج. وقد تم اخترق موقع الويب الحكومي الخاص بالمحافظة الشمالية وموقع الويب الحكومي الخاص بالسياحة في البحرين إلي جانب مواقع أخري عديدة. وكانت صور المصابين من المتظاهرين المعارضين للحكومة تظهر إذا قام أحد المستخدمين بالنقر على أحد الفئات الموجودة على الصفحات الرئيسية لكلا الموقعين.

ابريل ٢٠١١،اختراق موقع الويب الخاص بانتخابات أعضاء مجالس البلدية في السعودية

لقد نجح القرصان في اختراق موقع الويب وكان قادرًا على تغيير الصفحة الرئيسية للموقع وإضافة رسالة موجهة للملك عبد الله بن عبد العزيز مُطالبًا بالمساعدة للتخلص من ظلم أنظمة المرور في مدينته، قائلاً أنه قد عانى من الظلم كثيرًا ووصلت به الأمور إلي حد الإفلاس!

القطاع المالي:

مايو ٢٠١١، هجوم متصيد على بنك HSBC في مصر

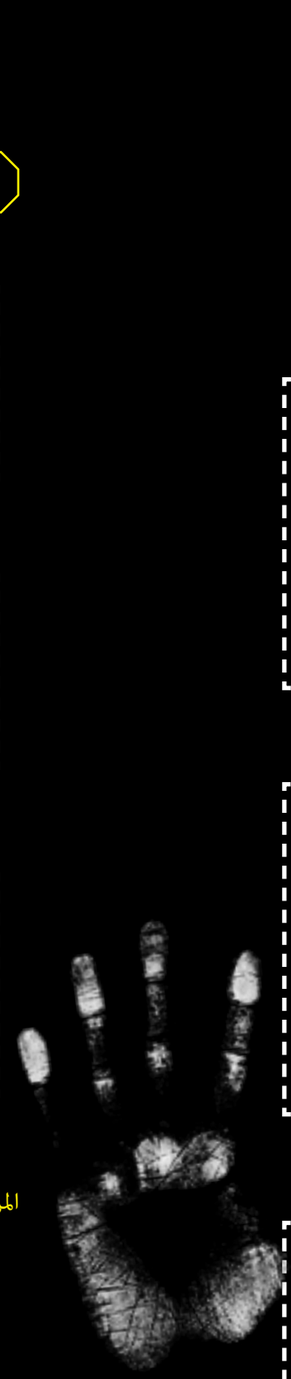
لقد تم إرسال بريد الكتروني خداعي من customer_service@hsbc.eg بعنوان: «تحديث حسابك». وتطلب هذه الرسالة من المستخدم أن يقوم بالنقر علي الرابط المُرفق بالبريد لاستلام رسالة عاجلة، وإلا سيتم حظر استخدام حسابه المصرفي علي الانترنت.

ابريل ٢٠١١، مصرف أبو ظبي الإسلامي

لقد تم إرسال بريد الكتروني خداعي من customerservice@adib.ae بعنوان: «إشعار أمني» يطلب من المستخدم إتباع رابط مُعين ليتمكن من استخدام قاعدة البيانات الوصلات الآمنة (SSL) الجديدة للبنك بدلا من القديمة

بنك دبي فيرست (Dubai First)

لقد تم إرسال بريد الكتروني خداعي من service@dubaifirst.com بعنوان: «تم حظر حسابك المصرفي عبر الانترنت» مع رابط مُرفق لإعادة تنشيط الحساب. وكما هو الحال في جميع الهجمات الخادعة أو الهجمات المعروفة بهجمات اصطياد المعلومات، فإن الرابط المُرفق يأخذك إلى موقع الويب الخاص بالقرصان وليس إلى موقع الويب الحقيقي للبنك.



المراجع

http://egyptianchronicles.blogspot.com/2011/06/akhbar-al-youm-website-is-hacked.html
http://egyptianchronicles.blogspot.com/2011/03/ontv-website-is-hacked.html
http://www.aljazeera.net/NR/exeres/07E58207-E080-414F-9C52-5C7D57CB6205.html
http://www.tradearabia.com/news/IT_200063.html
http://pastebin.com/n98jDJMq
http://www.tech-beat.com/719/
http://www.fraudwatchinternational.com/phishing/individual_alert.php?fa_no=239311&mode=alert
http://www.fraudwatchinternational.com/phishing/individual_alert.php?fa_no=239214&mode=alert
http://www.fraudwatchinternational.com/phishing/individual_alert.php?fa_no=239048&mode=alert

مقابلة مع

جو سوليفان

مدير قسم أمن المعلومات في موقع Facebook.com

أجرى الحوار: معتز صلاح

يُعد موقع Facebook اليوم من أحد أكثر مواقع الويب شهرة في كافة أنحاء العالم، وخصوصًا في الشرق الأوسط. وهو أحد أكثر الأمثلة المعروفة لظاهرة «الشبكات الاجتماعية»، حيث يُمكن للمستخدمين مشاركة معلوماتهم وتاريخهم الشخصي طُوعًا، ومشاركة قصص وتحديثات عن حياتهم اليومية، بالإضافة إلى مشاركة صور العائلة والأصدقاء، وعلاقتهم، والمزيد. ومع كل هذا القدر من المعلومات التي يتم مشاركتها على الشبكات الاجتماعية، والعديد من الاختراقات وسرقة البيانات، فقد أصبح الاهتمام بخصوصية موقع الـ Facebook أمرًا هامًا وشاغلاً أساسيًا.

ويُنسب أيضًا إلى موقع الـ Facebook (Facebook.com) الفضل في لعب الدور الرئيسي في الثورات العربية في الأشهر القليلة الماضية. وقد دفعت زيادة استخدام موقع الـ Facebook وتأثيره على الشعب بعض المؤسسات مثل الجيش المصري والوكالات الحكومية الأخرى لإنشاء صفحات رسمية على موقع الـ Facebook.

ولهذا السبب كان يجب على فريق سيكيوريتي كايزن (Security Kaizen) عقد هذه المُقابلة مع مدير قسم أمن المعلومات في موقع الـ Facebook (Facebook.com)، أ/ جو سوليفان، ومُحاولة التعرُف على المزيد من التفاصيل حول الموقع. ولقد قام معتز صلاح، رئيس تحرير مجلة سيكيوريتي كايزن (Security Kaizen) بمُقابلة جو سوليفان وقام بتوجيه الأسئلة التالية له.

هل يُمكنك تقديم نفسك إلى قُراء سيكيوريتي كايزن (Security Kaizen)؟

أنا جو سوليفان، مدير قسم أمن المعلومات في موقع الـ Facebook. أنا أقوم بإدارة بعض الفرق على موقع الـ Facebook والتي يتركز هدفها حول التأكد من تمتع الأشخاص الذين يقوموا باستخدام الموقع بتجربة آمنة وإيجابية.

وقد أمضيت ٦ سنوات في العمل في عدد مختلف من الوظائف الأمنية والقانونية في موقع باي بال (PayPal) وموقع ايباي (eBay) قبل انضمامي إلى موقع الـ Facebook في سنة ٢٠٠٨. ولقد عملت قبل ذلك في وزارة العدل الأمريكية لمدة ٨ سنوات. ولقد كنت محظوظًا جدًا لحصولي على فرصة لأكون المُدعي الاتحادي الأول في مكتب المُدعي العام الأمريكي وتكريس وقتي بالكامل لمحاربة جرائم التكنولوجيا. فقد حظيتُ بالعمل على العديد من قضايا الإنترنت البارزة والمعروفة، بدءًا من جوانب الأدلة الرقمية في التحقيق الخاص بأحداث الحادي عشر من سبتمبر (١١/٩) إلى قضايا مُستغلي الأطفال، وقضايا اختراق أجهزة الكمبيوتر، وقضايا التجسُس الاقتصادي. وقد كنت أيضًا من أحد الأعضاء المؤسسين لـ «وحدة الملكية الفكرية وقرصنة الحاسب الآلي» (Computer Hacking and Intellectual Property Unit)، وهي وحدة خاصة مقرها في وادي السيلكون مُخصصة لملاحقة جرائم التكنولوجيا على وجه الحصر.

هل يُمكنك أن تقديم نبذة عن فرق أمن المعلومات في موقع الـ Facebook وعن دور كل فريق ومتوسط عدد العاملين في كل فريق؟

يوجد لدينا أكثر من 30 شخصًا في فريق أمن المعلومات، ولكن هذا يُقلل حقًا من عدد الأشخاص الذين يعملوا في مجال أمن المعلومات في الشركة. فيوجد لدى موقع Facebook فرق هندسية، وفرق إدارة المخاطر، وفرق الامتثال وفرق العمليات خارج مجال أمن المعلومات ولكنها مُخصصة ١٠٠٪ للحماية وأمن المعلومات. ومعًا يقوم المئات منا بالتركيز على المنطقة. ففي داخل فريق أمن المعلومات، ننقسم إلى مجموعات فعالة مثل مجموعة حماية المنتجات، ومجموعة التحقيقات، ومجموعة ممارسات أمن المعلومات، ومجموعة تطبيق القانون.

ما هو نوع الأنشطة اليومية التي تتعامل معها؟

إن مجال أمن المعلومات في موقع الـ Facebook لديه مجموعة كبيرة من الواجبات بدءًا من الحفاظ على البيئة المادية الخاصة بالموقع وحماية البيانات الإلكترونية للمساعدة في الحفاظ على سلامة الموقع. فنحن نقوم بالعمل داخليًا على تطوير معايير حماية المنتجات وتعزيزها، والمشاركة خارجيًا لتعزيز حماية الممارسات عبر الإنترنت، وتنسيق تحقيقات داخلية مع وكالات تطبيق القانون الخارجية للمساعدة في تنفيذ ما يُقضي إليه الحُكم على الأشخاص اغلمسئولين عن رسائل البريد المزعجة، والتجسس، وعمليات الاحتيال، وغيرها من الإساءات.

ما هو الحدث الأكثر تحديًا الذي واجهته في الفترة الأخيرة؟

تأتي أكبر التحديات التي نواجهها عندما يجب علينا إثبات بُطلان السلبيات. فتجد العديد من «متخصصي» أمن المعلومات يقومون بالكتابة عن موقع الـ Facebook، ولكننا نقوم بالرد في الحال على نقاط الضعف المزعومة والتي تتضح في نهاية الأمر لتكون نظرية في أغلب الأحوال. ففي الشهر الماضي فقط كانت هناك قصتان حظت بتغطية وسائل الإعلام العالمية وإذا كنت قد قرأت العناوين الرئيسية عندئذٍ، كنت ستعتقد أن اختراقات حماية كبيرة قد تمت بالفعل. وفي الواقع، لم تُسبب نقاط ضعف الحماية الضرر لأي شخص في أي حالة.

نحن نقوم أيضًا بالتعامل مع تحديات فريدة من نوعها والتي تتطلب السرعة والابتكار. فقد حضر الموقف في تونس إلى ذهني (عندما قام مزودي خدمة الإنترنت بإدراج رمز في صفحة تسجيل الدخول الخاصة بالموقع)، لأنه شيء لم نتعرض له ولم نرهُ من قبل، ولكننا كنا قادرين على نشر خطة كاملة لمعالجة الحادثة في أقل من خمسة أيام (بما في ذلك إطلاق تغييرات في الترميز عبر الموقع).

هل تطلُب منك الحكومات المختلفة بما في ذلك الحكومة الأمريكية المساعدة في قضايا جرائم إلكترونية بعينها؟ وهل يُمكنك تقديم بعض الأمثلة على ذلك؟

يقوم عضوًا من أعضاء فريقي بالتحدث تقريبًا كل يوم أسبوعيًا إلى أحد مسئولي أحد الحكومات في مكانٍ ما حول العالم – وهذا يجب ألا يكون مفاجأة. وتتراوح هذه المجموعة من التفاعلات بين المشاركة النموذجية لاتجاهات الجريمة الإلكترونية، وللمشاركة في التحقيقات، وللحوار حول معايير المحتويات، وللاستجابة إلى طلبات الحصول على سجلات المستخدم. نحن نقوم بمحاولة تعزيز الحوار الإيجابي حتى نتمكن من فهم اهتمامات الحكومة بينما نحافظ دائمًا على التزامنا باحترام خصوصية وحقوق حماية مستخدمي الموقع.

ما هي خطة العمل التي قمت بوضعها أثناء الأحداث الأخيرة في الشرق الأوسط عندما قامت بعض الدول بحظر موقع الـ Facebook؟

لقد كان اهتمامنا الرئيسي طوال هذا الوقت هو الحفاظ على حماية الحسابات وسلامتها. فنحن لا يُمكننا معارضة أحد قرارات إيقاف الوصول إلى الإنترنت تمامًا أو حظر الوصول إلى موقعنا ولكن يُمكننا التركيز على منع الوصول غير المُصرح به إلى الحسابات.

ولتجنب الأحداث المُشابهة في المستقبل، ما هو نوع التحديثات التي قمت بوضعها في خطة الطوارئ الخاصة بك؟

نحن نقوم بالتركيز باستمرار على التدابير اللازمة لإعطاء الأشخاص التحكم الكامل في حماية حساباتهم. فقد قمنا بإطلاق بروتوكول نقل النص الفائق الآمن (HTTPS) المُدرج ونأمل في أن نجعل هذا البروتوكول (HTTPS) بروتوكولاً افتراضيًا للموقع قريبًا. ونُقدم الآن «إشعار تسجيل الدخول» و«موافقات تسجيل الدخول» [وهو نموذج ذو عاملين مزدوجين للتوثيق]، والتأكيد الاجتماعي، و كلمات مرور المرة الواحدة، والتحكم في الجلسات عن بُعد لتقديم أدوات الحماية اللازمة لحماية حسابات مستخدمي موقعنا. ولإكمال الأدوات التي تواجه المستخدم، نقوم بمراجعة أنظمتنا التقنية باستمرار والتي تتكون من برامج خاصة متعددة تقوم بتصنيف الإجراءات الضارة، وحجز الحسابات المنقوصة، وفحص عناوين مواقع الإنترنت (URLs) والمحافظة على سلامة الموقع.

هل لاحظت وجود هجمات على حسابات المتظاهرين أو على مجموعات بعينها خلال هذه الفترة سواء من الحكومة المصرية السابقة أو الحكومة التونسية؟

لقد كان أحد الجوانب المُضيئة في كل هذه الأحداث، أن الأدوات ذاتها التي قمنا بنشرها منذ سنوات لمنع تّصيُّد المعلومات وغيرها من عمليات الاستيلاء على الحسابات تعمل بشكل مُساوٍ وجيد في مكافحة محاولات الأنواع الأخرى في تسوية الحسابات. ولكن احترامًا لخصوصية كل مستخدم، لم نقم بمناقشة قضايا محددة علنًا.

هل تعتقد أن الحكومات لديها الحق في قطع اتصالات الإنترنت. وفي اعتقادك ماذا سيكون رد فعل المواطنين الأمريكين في هذه الحالة؟

من خلال نموذنا كخدمة يستخدمها مئات الملايين من الأشخاص في كافة الدول حول العالم، فقد أظهرنا قوة الإنترنت كأداة اتصال أساسية لا غنى عنها. لدرجة أننا نؤمن أن وسائل الاتصال والوصول إلى المعلومات أساسيان للوصول إلى مجتمع عادل، ويجب أن نقلق دائمًا في حالة انقطاع الإنترنت أو رفض الوصول إليه.

شكرًا،

جو

مقابلة مع

آل برمان

المدير التنفيذي لمؤسسة DRII الدولية

أجرى الحوار: معتز صلاح وعمر شيرين

هل يُمكنك تقديم نفسك لقُراء سيكيوريتي كايزن (Security Kaizen)؟

أنا أعمل كمدير تنفيذي لمؤسسة DRI الدولية منذ خمس سنوات. وقد عملت قبلها كرئيس لإدارة استمرارية العمل العالمية لمؤسسة مارش (Marsh) وقبلها كنت مدير تنفيذي لمؤسسة برايس ووترهاوس كوبرز (PwC). وبالإضافة إلي ذلك، بجانب عملي السابق كمدير تنفيذي، فقد كنت أيضًا المدير التنفيذي للمعلومات في أحد أكبر البنوك

هل يُمكنك أن تحدثنا عن مؤسسة DRI الدولية كمنظمة والدور الذي يقوم به أعضائها في مختلف الصناعات والمهن؟

إن مؤسسة DRI الدولية هي منظمة لا تهدف إلى الربح، وقد كَرست جهودها خلال الـ ٢٣ عامًا الأخيرة للإعداد ضد الكوارث حول العالم. فنحن نُعد أكبر مؤهلين ومدربين للأشخاص في مجال استمرارية العمل (BC).ونُقدم أيضًا الخدمات لمختلف اللجان حول أنحاء العالم. فنحن نقوم بالتدريس في ٤٥ دولة، باستخدام ثمانِ لغات، ولدينا حوالي ٨,٥٠٠ متخصص معتمد في أكثر من ١٠٠ دولة في كافة الصناعات والمهن.

هل تلعب مؤسسة DRI الدولية دورًا في دعم المؤتمرات التي تهتم باستمرارية العمل ومعالجة الكوارث (BC/DR)؟

تلعب مؤسسة DRI الدولية دورًا في المؤتمرات في كافة أنحاء العالم. في الواقع، لقد عُدت مؤخرًا من أحد المؤتمرات في البرازيل والذي خصص أحد أيامه (DRIDAY) للمتخصصين المعتمدين من مؤسسة DRI لمناقشة أدوارهم في منظماتهم. وسوف أحضر مؤتمر آخر في بروكسيل ببلجيكا نهاية شهر يونيو. وقد شَاركت مؤسسة DRI في مؤتمرات مختلفة في اسبانيا والمكسيك وسنغافورة والولايات المتحدة وماليزيا خلال عام ٢٠١١ فقط. وفي عام ٢٠١٢، ستقوم مؤسسة DRI الدولية بعقد مؤتمرها الخاص في شهر مايو في مدينة نيو أورليانز الأمريكية.

هل يُمكنك أن تُخبرنا عن التطورات وعن رؤيتك الخاصة فيما يتعلق بالأحداث الأخيرة التي تركزت حول القوانين والمعايير الخاصة باستمرارية العمل (BC) في العالم؟

لقد شهدنا قوانين ومعايير جديدة حول العالم في مجال استمرارية العمل (BC)، وقد تبين أن معظمهم كان رد فعل لأحد الأحداث. وتُعد أحداث الحادي عشر من سبتمبر (١١/٩) دافعًا كبيرًا للتطوير في الولايات المتحدة، ولكن يُمكننا رؤية تأثير هذه الأحداث في كافة أنحاء العالم. فيوجد لدى كل بنك مركزي متطلبات لاستمرارية العمل (BC). وتوجد معايير بريطانية (BS 25999) ومعايير أمريكية (NFPA 1600) وتوجد أيضًا معايير أخري مختلفة. وسيكون المعيار المطور الجديد ISO 22301 محاولة لإنشاء معيار عالمي للجودة (ايزو - ISO) ليحل محل المعيار البريطاني BS25999.

لكننا بدأنا نري قوانين جديدة ناتجة عن الأحداث الرئيسية. فمثلاً إذا نظرنا للأحداث الأخيرة في الولايات المتحدة فسنجد أن مشروع قانون Dodd-Frank Bill - الذي يتعامل مع الأزمة الاقتصادية - يحتوي علي مبادئ استمرارية العمل. وقد أقرت أيضًا الهيئة الرقابية للقطاع المالي (FINRA) - التي تُعتبر أساس الرقابة المالية في الولايات المتحدة - قانون 4370، الذي يشمل أيضًا مبادئ استمرارية العمل (BC).

ولكن ما نشهده حقًا هو الفهم الحقيقي أن شركات الأعمال يجب أن تكون مُهيأة للطوارئ, ويجب أن يمروا

بمراحل التخطيط لكي يستطيعوا أن يحافظوا ليس فقط علي سلامة وتطور مشروعاتهم ولكن أيضًا للمحافظة علي من يعملون معهم. فعلى سبيل المثال، قد أظهرت الأحداث الأخيرة في اليابان مدي تأثير الأحداث علي سلاسل الإمدادات في العالم كله.

هل تعتقد أن المعايير الجديدة الخاصة باستمرارية العمل ومعالجة الكوارث (BC/DR) ستُعطي اهتمامًا أكبر لمعالجة بيئة التكنولوجيا بما أن معظم المعايير القديمة لم تقُم بذلك تاريخيًا؟

أعتقد أن هناك العديد من المعايير الخاصة بالتكنولوجيا، فتجد مثلاً أن معيار ISO 27001 مُركز كليًا على التكنولوجيا. ولكني أعتقد أنك قد تكون محقًا إلي حدٍ ما. فمعيار الايزو الجديد (ISO 22301 سيحل محل المعيار البريطاني BS 25999. وكما تعرف، فإن المعيار البريطاني BS 25999 لا يحتوي علي مبادئ معالجة قطاع تكنولوجيا المعلومات (IT). ولذا، فأنا أعتقد أن هناك فهم كبير أن التكنولوجيا تلعب دورًا أساسيًا وهامًا للمساعدة في معالجة كافة العمليات.

برأيك ما الذي سيقوم المعيار الجديد ISO 22301 بتطويره والاهتمام به مقارنةً بمعيار الجودة البريطاني BS-25999 الحالي؟

أعتقد أنهم سيولوا معالجة مجال التكنولوجيا اهتمامًا أكبر, وهذا غير موجود في معيار الجودة البريطاني BS-25999. وأعتقد أيضًا أنه سيكون ذو قاعدة عريضة صالحة للاستخدام العالمي - لكونه معيار عالمي - عكس المعايير البريطانية المُتشددة. وسيوفر إطارًا أوسع للعمل. ولذا، أظن أنه سيكون تطورًا كبيرًا عن المعيار البريطاني BS 25999.

ولكن كما يعرف معظمنا, فإن المعايير ليست بقوة القوانين .وأعتقد أيضًا أننا سنرى المزيد من القوانين قريبًا. وبالنظر إلى القوانين، ستجدها إلزامية ولذا فهي تُخبرك بما يجب عليك القيام به. وهي قائمة علي أسس الأداء، ولذا فهي تُخبرك بكيفية قياس ما تقوم به. والمعايير، وحدها، لا تقوم بذلك. فهي تعمل فقط كأساس للمقارنة، بين أفضل المُمارسات وبما تقوم به في منظمتك.

هل تعتقد أن المنظمات التي تستخدم مفهوم السحابة (Cloud concept) ستكون مُتقدمة خاصةً بعد الأحداث الأخيرة في الشرق الأوسط وأيضًا كارثة الزلزال في اليابان؟

أعتقد أن ما يقوم به مفهوم السحابة (Cloud concept) هو إبعادك عن حادث مُعين بحيث لا يؤثر علي مسار عملك. إن ما رأيناه في اليابان على وجه الخصوص، هو قدرة النظام المالي علي استمرار العمل حتى في الأماكن التي دمرها الإعصار. ولذا، بالطبع سيكون مفهوم السحابة (Cloud concept) مُتقدم.

ومع ذلك، فإن واحدة من أكبر المشاكل في الشرق الأوسط بعد الاضطرابات الأخيرة في مصر هي انقطاع الانترنت. إن انقطاع الإنترنت لم يكن ليساعدك علي استمرار الأعمال حتى لو كان لديك تكنولوجيا السحابة (Cloud technology). ولذا، ما دامت وسائل الاتصالات متاحة، فإن تكنولوجيا السحابة (Cloud technology) بالتأكيد هي أفضل الطرق لإدارة الأعمال، وخصوصًا في الأزمات.

في أعقاب الأحداث الأخيرة في الشرق الأوسط، كيف يُمكنك تحديد الأولويات ذات الأهمية الأكبر التي يجب أن تهتم بها المنظمات في المنطقة؟

بالتأكيد إن أول اهتماماتنا هي الناس, ولكنني أعتقد أن التكنولوجيا هي عنصر كبير جدًا نحتاج إليه. ولذا، يجب أن نتأكد أن التكنولوجيا متاحة لنستطيع التواصل داخل الدولة وخارجها. أعتقد أننا في حاجة إلى أن نتفهم أهمية وضع خطط ووجود موارد يُمكنك استخدامها بعيدًا عن المنطقة المُتضررة. ولذلك، يجب علينا أن نهتم بوضع الخطط والأهم من ذلك أن يكون لدينا القدرة على اختبار مدي جودة الخطط التي وضعناها.

قامت العديد من المنظمات بالإبلاغ عن زيادة في عمليات الاحتيال بعد الأحداث الأخيرة، وخصوصًا العمليات التي تندرج تحت بند غسيل الأموال. ما هي المخاطر ذات الصلة التي يجب أن تهتم بها المنظمات وتأخذها بعين الاعتبار في أوقات الأزمات؟

في أوقات الأزمات، نميل إلي استخدام المنشآت غير المؤمّنة وغير المحمية كال المنشآت التي نستخدمها في أوقات وعمليات اليوم بيوم العادية. ولذلك، يجب أن نتأكد من تأمين تلك المنشآت، بما في ذلك تكنولوجيا السحابة (Cloud technology)،يساوي - إن لم يكن أفضل - الحماية العادية. ويجب أن يكون لدينا بُعد نظر. وأحد الأشياء التي ننساها عادةً هو وجود فريق متاح للتدقيق والمراجعة ليحاول فهم تطورات الأحداث. وفي أوقات الأزمات، يجب علينا توقع أن هناك من سيحاول القيام بعمليات احتيال والاستعداد لتلك العمليات.

برأيك ما الذي سيقود إلى تبني ثقافة استمرارية العمل ومعالجة الكوارث (BC/DR) في منطقة مثل منطقة الشرق الأوسط حيث لا يوجد قوانين ولوائح للإدارة؟

حسنًا، لقد شهدنا بعض التطورات في المنطقة مؤخرًا. أعتقد أننا إذا نظرنا إلي البنك المركزي لأي دولة شرق أوسطية، فسنجد به مبادئ استمرارية العمل ومعالجة الكوارث (BC/DR). لكن ما سيقود إلي زيادة استخدامها هي الشركات وخاصة الشركات الخارجية التي تفكر في القيام ببعض الأعمال في الشرق الوسط والتعامل مع الموردين في المنطقة. يجب أن يصل هؤلاء الموردين إلي مستوي أداء مماثل للمعايير الدولية. أعتقد أن الدافع لذلك سيكون الأعمال لكني أعتقد أن الشركات أظهرت أنها سوف تذعن لقوانين المنطقة التي تتواجد فيها. ولقد اكتشفنا انك يجب أن تمتلك مبادئ استمرارية العمل (BC) لكي تستطيع الاستمرار في تطوير أعمالك وشركاتك.

هل يُمكن للسحابة أن تُنقذ شركتك من كارثة؟؟

بقلم: محمد توفيق

لقد أصبحت الحوسبة السحابية اتجاهًا هامًا في التكنولوجيا ويتوقع العديد من الخبراء أن الحوسبة السحابية ستُعيد تشكيل مجال تكنولوجيا المعلومات (IT).
ووفقًا للدراسة التي قامت بها مؤسسة فورستر مؤخرًا مع ٢٨٠٣ من صانعي القرار في مجال تكنولوجيا المعلومات (IT)، فإن تطوير إمكانيات مجال استمرارية العمل ومعالجة الكوارث (BC/DR) له الأولوية عند الشركات الصغيرة والمتوسطة كما يُعتبر من ثاني أهم الأولويات بالنسبة للشركات الكبرى خلال الأشهر الاثنى عشر المُقبلة.
وأيضًا في نطاق برامج استمرارية العمل ومعالجة الكوارث (BC/DR) يتم تطوير: برامج مُطورة، ومُعدة لتُناسب جميع المشاكل التي تسبب الأعطال – بما في ذلك انقطاع الكهرباء والأعطال التي تُسببها الأحوال الجوية – وليس فقط الكوارث النادرة الحدوث. يجب أن يستفيد متخصصي الأمن والسلامة من هذه التطورات الواضحة كما تقوم معالجة الاقتصاد بتخفيض ميزانيات تكنولوجيا المعلومات ببطء لتحسين تطوير تنظيم وعمليات مجال استمرارية العمل ومعالجة الكوارث (BC/DR).
يُشير التقرير "تَصَدُر استمرارية العمل ومعالجة الكوارث (BC/DR) أعلى أولويات تكنولوجيا المعلومات لعام ٢٠١٠ و٢٠١١" بأن ٣٢٪ من الشركات الكبري و٣٦٪ من الشركات الصغرى والمتوسطة تُخطط لزيادة إنفاقها علي استمرارية العمل بما لا يقل عن ٥٪، بينما يُخطط ١١٪ فقط من الشركات الكبري و٨٪ من الشركات الصغري والمتوسطة لخفض إنفاقها على استمرارية.

تُشير هذه الإحصاءات إلى أن الشركات تتطلع إلى المصداقية. فتجد أن البنية التحتية للسحابة تُمثل تحولاً نموذجيًا في مجال استمرارية العمل ومعالجة الكوارث (BC/DR). وتتطلع الشركات إلى حلول فعالة وغير مُكلفة للمصداقية، وتقوم الحوسبة السحابية المُصممة بشكل جيد بجعل العديد من المواقع الزائدة عن الحاجة مناسبة للاستخدام في استراتيجية استمرارية العمل ومعالجة الكوارث (BC/DR) الشاملة.

وفي اكتوبر ٢٠١٠، قامت مجموعة ابردين (Aberdeen) بإجراء استطلاع للرأي لأكثر من ١٠٠ منظمة تستخدم برامج رسمية لمعالجة الكوارث (DR) لمعرفة ما اذا كانوا يقوموا باستخدام برنامج عام للتخزين على السحابة، وإذا كان الأمر

كذلك، مل هي الفوائد التي ظهرت في أدائهم. وقد اكتشفت مجموعة ابردين (Aberdeen) أن المنظمات التي نقلت علي الاقل جزءًا من بياناتها إلى السحابة عالجت المشاكل الناتجة عن الأحداث بـ 4 أضعاف سرعة المنظمات التي لا تملك برنامج تخزين رسمي على السحابة. وبالإضافة إلى ذلك، فقد استطاع مستخدمي برامج التخزين على السحابة تحقيق أهداف الاسترجاع الزمني أكثر ممن يقوموا بتخزين بياناتهم في أجهزة الكمبيوتر.

إن حلول استمرارية العمل ومعالجة الكوارث (BC/DR) المعتمدة علي السحابة مناسبة لأي شركة لا يُمكنها تحمل الأزمات وفقدان البيانات، ولكن هذا لا يضمن أنه لن يكون هناك انقطاع في الخدمات. فمثلاً فقد حدث في شهر ابريل انقطاع كبير ونادر الحدوث في خدمات الويب المعتمدة علي السحابة الخاصة بـ Amazon وقد تسبب ذلك في انقطاع عدد كبير من مواقع الإنترنت الأخرى مثل Reddit، و HootSuite، وFoursquare، وQuora.

فإن الاهتمام الأساسي بالحوسبة السحابية هي مسائل خاصة بأمن المعلومات والخصوصية التي صُنفت لتشمل الوصول إلى بيانات حساسة، وعزل البيانات، واستثمار الاخطاء، والمعالجة، والمحاسبة، ومواجهة الدخلاء الخبيثين، وحماية وحدة التحكم الخاصة بالإدارة، والتحكم بالحساب، و تعدد الإيجار.

وتتضمن الحلول لمشاكل أمن معلومات السحابة المتنوعة استخدام عدد أكبر من الأكواد وخصوصًا البنية التحتية للمفتاح العام (PKI)، واستخدام العديد من مزودي السحابة، وتوحيد مقاييس واجهة برمجة التطبيقات(API)، وتحسين الآلات الافتراضية والدعم القانوني.

وقد قام "منتدي السحابة المصرية" (Egypt Cloud Forum) بتنظيم يوم السحابة المصري لزيادة الوعي بالحوسبة السحابية والقضايا الأمنية ذات الصلة. إن "منتدي السحابة المصرية" (Egypt Cloud Forum) هو التابع الرسمي لتحالف أمن معلومات السحابة (Cloud Security Alliance) في مصر مع تركيز المنتدى على "تحديد نقاط ضعف السحابة وأمن المعلومات الافتراضي".

وتُعد منظمة "تحالف أمن معلومات السحابة" (CSA) منظمة غير هادفة للربح، وتهدف إلى تطوير استخدام أفضل الممارسات لتوفير ضمان أمن المعلومات في مجال الحوسبة السحابية، ولتوفير تعليم كيفية استخدام الحوسبة السحابية للمساعدة في تأمين أشكال الحوسبة الأخرى.ويقود منظمة "تحالف أمن معلومات السحابة" ائتلاف واسع من العاملين بالصناعات والشركات والمؤسسات وأصحاب مصالح رئيسية آخرين.

egypt CLOUD FORUM

المصادر

http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm
http://www.forrester.com/rb/Research/business_continuity_and_disaster_recovery_are_top/q/id/57818/t/2
http://www.cloudsecurityalliance.org
http://www.egyptcloudforum.com/?q=node/42
http://www.aberdeen.com/aberdeen-library/6827/RA-disaster-recovery-cloud.aspx
http://www.aberdeen.com/aberdeen-library/6827/RA-disaster-recovery-cloud.aspx

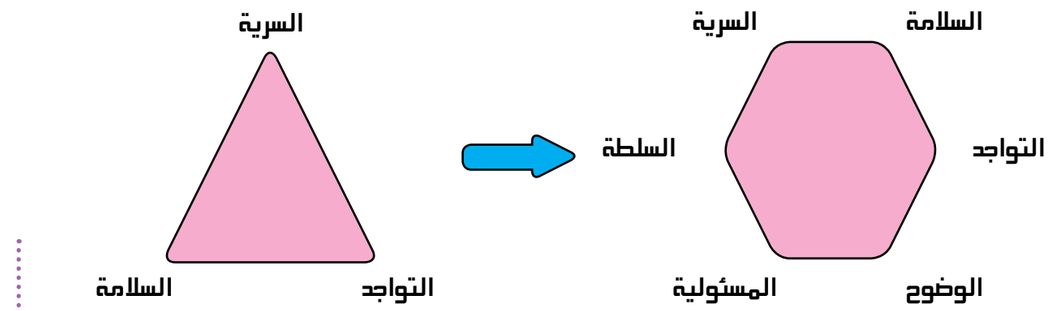
النهج المستقبلي لضمان حماية البيانات في السحابة

بقلم: فينوث سيفا سوبرامانيان ومحمد محي الدين

لقد قطعت تكنولوجيا المعلومات شوطًا كبيرًا منذ اختراع أجهزة الكمبيوتر. وقد قطع مجال أمن المعلومات شوطًا كبيرًا أيضًا. فقد ساعدت الاتجاهات مثل اتجاه «الحوسبة السحابية» المستثمرين والمبتكرين الصغار والمتوسطين (SMIs) من خلال تقليل التكلفة المبدئية للانتشار والصيانة. وهذا بالتأكيد سيُمهد طريقًا جديدًا للعديد من الأشخاص. وباستخدام الاتجاهات الناشئة مثل اتجاه «حماية البيانات في السحابة» والتي يجب ألا يتم النظر إليها بالشكل التكاملي الثلاثي التقليدي ولكن يجب النظر إليهم بطريقة جديدة.

وسيُناقش موضوعنا هذا طرق كيفية إمكان تغيير نموذج حماية البيانات في المستقبل القريب وطرق التعامل مع النماذج الجديدة.

وكما جرت العادة فإن أمن المعلومات يخضع إلى مثلث أمن المعلومات الرئيسي ("CIA triad")، أي السرية والسلامة والتواجد، ولكن هذا مُلزم بالتغيير في المستقبل خصوصًا مع انتشار البيانات في كافة انحاء العالم. و سيوفر هذا النموذج مستوى عالٍ من حماية البيانات وتوثيقها:



وبما أن المواد موجودة بشكل كافٍ والموارد متاحة بالفعل للتعامل مع المعايير الثلاث الأولى مثل السرية والسلامة والتواجد فسوف نُركز اهتمامنا على المعايير الثلاثة الأخرى وهي الوضوح والمسئولية والسلطة. وسنقوم بتركيز هذا المقال على منظور المعالجة والسلطة.

وتكون اتفاقية مستوى الخدمة (SLA) الواضحة والمحددة جيدًا هي أول خطوة لضمان حماية بياناتنا. ونُقدم هنا بعض المناهج الجديدة لصياغة اتفاقية مستوى الخدمة (SLA) التي ستقوم بتنفيذ وضع مُربح لكلا الجانبين.

١. المسئولية:

وتُعد المسئولية أحد مفاهيم المعايير الأخلاقية والسلطة بالعديد من المعاني. ويستخدم هذا المفهوم بشكل مترادف مع مفاهيم مثل مفهوم الاختصاص ومفهوم المُساءلة. ومن وجهة النظر الإدارية الحديثة، يُمكن أن تُصاغ في كلمتين «قيادة مذهلة»، ويُمكن النظر إلى هذا الجانب إما من المنظور الشخصي أو من المنظور التنظيمي، حيث إن كلٍ من الأشخاص والمنظمات يسعون وراء نداء الواجب لإنشاء علاقات ناجحة ومستديمة. وها هي بعض العوامل التي يُمكن أن تنسج في اتفاقية مستوى الخدمة:

١,١ التواجد: ستقوم مسودة اتفاقية مستوى الخدمة (SLA) بكسب الحد الأدنى من الوقت الذي يُمكن للمنظمة الصمود فيه أثناء الاضطرابات. وذلك لأن بعض التطبيقات في المنظمة قد لا تكون مهمة مقارنةً بالتطبيقات الأخرى الأكثر أهمية. وبهذا الشكل يحصل العميل على جودة أفضل للخدمة الخاصة بتطبيقاته الأكثر أهمية. والنموذج الوارد أدناه هو قالب للنموذج الذي يُمكن استخدامه كجدلية:

اسم التطبيق	التواجد المطلوب	متوسط مدة التوقف
الخدمات المصرفية عبر الإنترنت	١٠٠	صفر
التطبيق HRMS	٩٩	ساعة واحدة

١,٢ المكافآت الإدارية: يُعد هذا شيئًا جديدًا، تقوم مسودات الاتفاقيات التي تنُص بوضوح على المكافآت التي ستقوم بمشاركتها مع المزود - إذا تم تحقيق الهدف النهائي المتمثل في مصداقية وأمن البيانات – بجعل هم يُدركوا المقاييس التي تحتاجها لحوافز المشاركة. ويُمكنك أيضًا توفير شهادات تميُز كمكافآت للأشخاص الذين يقوموا بالحفاظ على البنية التحتية والمساعدة في تحقيق تفوق وتميُز العمل.

١,٣ الخسارة في الأعمال التجارية: وتنُص الاتفاقية أيضًا بوضوح على المخاطر القانونية وغيرها من المخاطر التي سيتكبدها الوكيل إذا لم يُلبي المقاييس التي تُعتبر مناسبة للمنظمة، وستتراوح النتائج بين إلغاء العقود والغرامات التي يتم فرضها بسبب الالتزامات القانونية.

١,٤ توظيف الأشخاص: تقوم باكتساب ذلك النوع من الأشخاص الذين يجب توظيفهم لإدارة بياناتك والبنية التحتية الخاصة بك، ونوع الاختبارات التي يجب اختبارها على هؤلاء الأشخاص، وعلى وثائق الاعتماد (مثل المؤهلات والشهادات) التي يجب أن يكونوا قد حصلوا عليها.

١,٥ ممارسات السلطة الجيدة: وتضمن هذه الممارسات أن منظمة مثل مزود خدمة الإنترنت (ISP) سيقوم بممارسة مبادئ جيدة للسلطة بالإشارة إلى الإدارة، والتي تُعد الأساس لسلطة الشركة التي تمتد إلى ما وراء سلطة تكنولوجيا المعلومات. وتُتاح سلوكيات إرشادات السلطة الجيدة في الكتاب الأحمر (Red book) الخاص بمجموعة OCEG. والمنظمات التي تمارس سلطة جيدة هي القادرة على الاستمرار على المدى الطويل. وللاستشهاد بمثال، ففي حالة سعي مزود الخدمة (ISP) للاندماج أو الاستحواذ، يجب على مزود الخدمة (ISP) أن يضمن إعلام العملاء بشكل صحيح وأن يكون واضحًا بخصوص ما يحدث لبياناتهم.

١,٦ ممارسات تكنولوجيا المعلومات (IT) الجيدة: جعل ممارسات تكنولوجيا المعلومات تتحمل المسئولية لاتباع ممارسات تكنولوجيا المعلومات الجيدة مثل ITIL، وSAS70، إلخ. وهذا سيضمن لك أنه يتم التعامل مع بيانات بعناية وبشكل صحيح، بما أنه يتم مراجعة المنظمات التي يوجد لديها مُصداقات من قِبل هيئة مستقلة. وإن لم يكن هذا ممكنًا، فبإمكانك أن تجعل هذه الممارسات تتبع إجراءات «إدارة الحوادث»، و«إدارة التغيير»، و«إدارة الإطلاق»، و«إدارة المشاكل»، و«إدارة أمن المعلومات» وفقًا لمعايير ITIL أو وفقًا لأية معايير رائدة أخرى. وهذا سيضمن الثقة بين أصحاب المصالح بالإضافة إلى الإدارة.

٢. الوضوح:

إن أحد أكبر التحديات في الحوسبة السحابية هو إكساب الوضوح للبنية التحتية لمزود الخدمة.فستقوم منظمات عديدة بتوفير نوعًا من المُصادقة مثل معيار الجودة ISO 27001، ولكن هل يضمن هذا أنه سيتم الاهتمام بكل شيء؟ للأسف، لن يحدث ذلك. إذن كيف يُمكن لأي منظمة أن تعالج مشكلة الوضوح؟ ها هي بعض الخطوات للقيام بذلك:

٢,١ توفير فريقًا متخصصًا خاصًا بالمنظمة: قم بتوفير فريقًا صغيرًا متخصصًا خاصًا بالمنظمة متكون من مشرفين على النظام، أو مشرفين على الشبكة، أو موظفين لأمن المعلومات الذين يستطيعون تحديد نوعية البيانات وما إذا كانت هامة/هامة إلى حد ما/عادية ويستطيعون أيضًا مراقبة حركة نقل البيانات. الهدف من هذا الفريق هو الإبلاغ عن الانتهاكات ودخول الحالات الغريبة.

٢,٢ تطبيق المراقبة عن طريق كاميرات المراقبة (CCTV): من خلال المراقبة عن طريق كاميرات المراقبة (CCTV) يُمكن للعميل رؤية الإجراءات الأمنية لأماكن تواجد البيانات على أرض الواقع. قم بتسجيل الاستنتاجات، ومراجعتهم شهريًا، وكتابة الملاحظات، ونشرها وأرشفتها في ذاكرة خارجية. ستكون هذه الاستنتاجات مفيدة بخاصةً أثناء التعامل مع القضايا القانونية الناتجة عن العمليات التي تحدث في كافة أنحاء العالم.

٢,٣ إدارة الهويات والتحكم في عمليات الدخول: التأكد من أن مزودي الخدمة يقوموا بتقديم القدرة على تنفيذ امتيازات إدارة الهويات والتحكم في الوصول حسب احتياجاتك الخاصة وللأنظمة الهامة التي تتطلب تصديق ثنائي الهوية لتنفيذها حيث تتطلب التغييرات تصديق شخصين عليها. قم بتنفيذ التوثيق والتصريح والتدقيق (AAA) لهذه الأنظمة وتوفير تسجيل لهم على مركز خدمة سِجِّل النظام.

٢,٤ النسخ الاحتياطي: تُعد استمرارية العمل ومعالجة الكوارث (BC/DR) من العناصر الهامة للتواجد لكن المدير التنفيذي للمعلومات في حاجة إلى التأكُّد من امتلاك الحقائق المباشرة في بيانات النسخ الاحتياطي، مثل أماكن تواجدها، ومن الذي يُمكنه الوصول إليها، والطريقة التي يتم إدارة البيانات بها.

٢,٥ مركز خدمة تسجيل دخول التطبيقات: تطبيق مركز خدمة تسجيل الدخول حيث سيتم إدخال كل معاملات بنيتك التحتية وبياناتك على الخادم. يجب ألا تقم بتوفير الوصول إلى هذا الخادم لأيٍّ من مزودي الخدمة حيث إن الوصول إليه يجب أن يكون مصرحًا به لمجموعة محددة من العاملين داخل المنظمة، مثل المدير التنفيذي للمعلومات والمدير التنفيذي لأمن المعلومات فقط. تأكد أن الملفات المُدخلة للقراءة فقط ولا يُمكن تعديلها.

٣. السلطة:

يعتمد هذا المفهوم على نظرية «ثق ولكن تحقق». وعلى الرغم من الحصول على كل العوامل السابقة بشكل صحيح،

يجب على كلٍ من المدير التنفيذي للمعلومات والمدير التنفيذي لأمن المعلومات أن يعتمدوا أسلوب قائم على أساس المراجعة. ونحن نقدم هنا أساليب سلطة متعددة الجوانب.

٣,١ إدارة المخاطر: إجراء تقييم ربع سنوي للمخاطر يتم إجراءه بواسطة فريق أمن العلومات الداخلي الخاص بك تماشيًا مع المعايير الدولية مثل NIST أو COBIT. قم بتسجيل هذه الملاحظات ثم قم بنشرها.

٣,٢ تحليل نقاط الضعف و اختبار الاختراقات: إن إجراء تحليل لنقاط الضعف واختبار الاختراقات (VA/PT) نصف سنوي بواسطة فريقك الداخلي وآخر سنوي بواسطة فريق متخصص خارجي؛ سوف يساعد هذا على اكتشاف عناصر المفاجأة وتقليل المخاطر.

٣,٣ المراجعة الداخلية: إجراء مراجعة سنوية بواسطة الفريق الداخلي ومراجعة أخرى بواسطة فريق مراجعة خارجي متخصص. قم بتجميع المراجعات ومناقشة النتائج مع الإدارة العليا لمزودي الخدمة. وأيضًا قم بتحديد الاهتمامات ومجالات التحسين الممكنة ومعالجتهم بواسطة آليات التعويض المختلفة.

الاستنتاج: لقد وُجدت الحوسبة السحابية لتبقى وستُغير الطريقة التي من خلالها يتم إدارة البيانات وتخزينها ومعالجتها. وبإتباع الإجراءات السابقة يُمكن للمدير التنفيذي للمعلومات/مدير قسم أمن المعلومات التأكد من تحقيق مستوى عالٍ من تأمين البيانات. وتتطلب العمليات السابقة استراتيجيات جيدة التخطيط وميزانية وموارد كافية ولكن بالنظر إلى العائد على الاستثمار (ROI) الذي توفره الحوسبة السحابية يصعب أن ترفضها الإدارات.

الاستنتاج: لقد وُجدت الحوسبة السحابية لتبقى وستُغير الطريقة التي من خلالها يتم إدارة البيانات وتخزينها ومعالجتها. وبإتباع الإجراءات السابقة يُمكن للمدير التنفيذي للمعلومات/مدير قسم أمن المعلومات التأكد من تحقيق مستوى عالٍ من تأمين البيانات. وتتطلب العمليات السابقة استراتيجيات جيدة التخطيط وميزانية وموارد كافية ولكن بالنظر إلى العائد على الاستثمار (ROI) الذي توفره الحوسبة السحابية يصعب أن ترفضها الإدارات.

السيرة الذاتية: لقد عملت في مجال أمن المعلومات لمدة السبع سنوات الماضية وأعمل حاليًا كمدير لمراجعة تكنولوجيا المعلومات في صرافة الإمارات العربية المتحدة حيث إنني مسئول عن مراجعة وتوافق تكنولوجيا المعلومات.وأنا أيضًا مشتركمع «تحالف تأمين السحابة» كعضو كما أنني شغوف بسلطة وتوافق وأخلاقيات ومراجعة تكنولوجيا المعلومات. بالإضافة إلى كوني عضو عامل في لجنة «الأخلاقيات الإلكترونية الدولية» وعضو استشاري لـ «مجموعة توافق سياسة تكنولوجيا المعلومات» التي يُمكن الوصول إليها عن طريق البريد الإلكتروني vinoth.sivasubramanian@gmail.com.

يعمل محمد محي الدين كنائب رئيس الاستراتيجية وتوصيل الخدمات الخاصة بشركة Intrendz Consulting، وهي شركة للاستشارات التجارية متخصصة في التأمين والاستشارات الإدارية لتكنولوجيا المعلومات (IT) ويُمكن التواصل معه عن طريق بريده الإلكتروني: peermohamed.mohideen@intrendz.co.in

secureninja.com
Forging IT Security Experts

Secure Ninja provides expert Information Security training, certification & services.
Visit our Digital Dojo at secureninja.com to see if you qualify or call us at 703.535.8600.

CISSP | CEH v7 | CCNA | CISM | Security + | CAP | CISA | CHFI | ECSA | ISSEP | ISSAP | ISSMP | ECSA | Network+ | EDRP | ECSP