July / September 2012

Security kaizen MAGAZINE

CONTROL YOUR VULNERABILITIES

ONE Year of Success

BLUEKAIZEN.ORG

ملاحظات توعية
من فريق الفيس بوك

مقابله مع
دكتور / شريف هاشم
نائب رئيس ITIDA

أحداث
كايرو سيكيوريتي
كامب ٢٠١١

Fixed Solutions

DON'T MISS OUR SPECIAL OFFERS

End of year Discounts

Data is encrypted Using AES/TwoFish

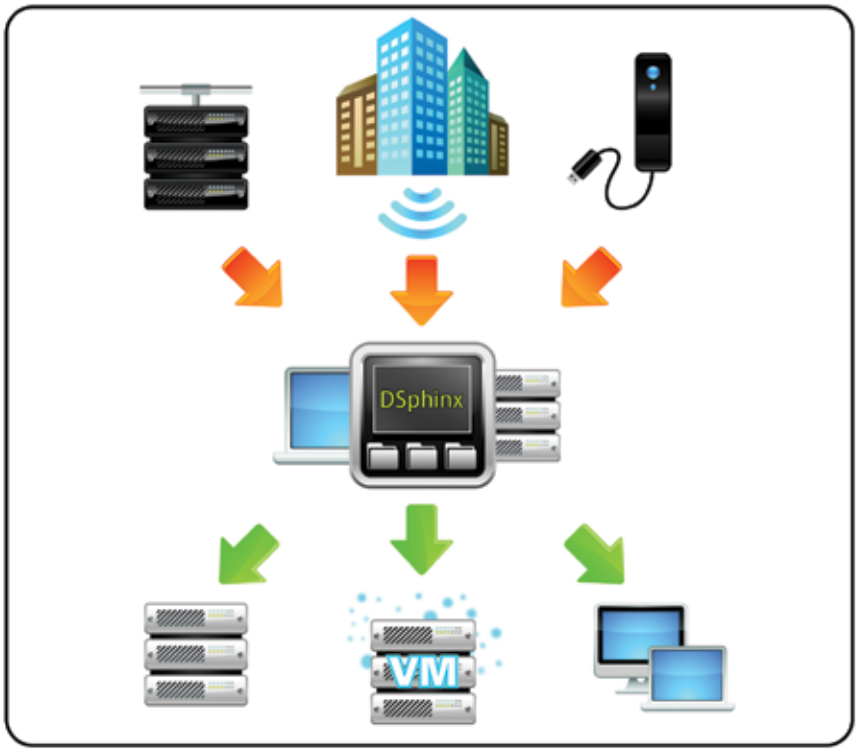
DSphinx

The Ultimate Backup Solution

Get your files securely anytime ... anywhere !

Download your trial version now

http://www.dsphinx.com



Cloud Backup Solutions

Cross Platform

+2 0222638292
+2 0222615685
Facebook.com/dsphinx
www.dsphinx.com
www.fixed-solutions.com

Contents

Editor's Note

1 year, 12 months, 365 days and 8760 hours had been passed since the release ....

True Story

Treachery, deceit and pilfering have always been associated with mankind ever since the Neanderthal age. History has been a sore witness ....

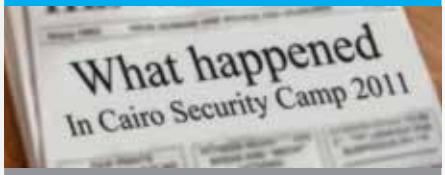
Grey HAT

It all started while being so hungry and trying to figure out what to eat ...

Awareness

Facebook Tips
At Facebook, we work hard to protect the people ...

New & News



For those who are not familiar with CSCAMP, it's an annual conference for information security professionals where we gather all security

Interview

With ... Dr. Sherif Hashem

Senior Advisor to the CIT Minister for CyberSecurity at Ministry of Communications ....

Best Practice

Constructing mature information security awareness and educational models,
Information Security is defined as protecting information and the systems that hold and support them directly from unauthorized use, access, disclosure, disruptions, modification and destruction. Any organization irrespective of their size and number util ...

SK Magazine Team

Security Kaizen magazine

Chairman & Editor-In-Chief
Moataz Salah

Editors
Hidayath Ullah Khan
Joe Sullivan
Sameh Sabry
Ahmed Nile
Omar Sherin
Vinoth Sivasubramanian
Naveen Sharma

Website Development
Mariam Samy

Translation
Mai Alaa El-Dein
Asmaa Ibrahim

Marketing Coordinator
Mahitab Ahmed

Photographers
Mohamed Mohsen
Mohamed Samy

Designed & Printed By
2DAY Adv.

改善
BLUE KAIZEN
Connecting Minds Improving Lives

كلمة المُحرر

لقد مرت عام، اثنا عشر شهرًا، 365 يومًا و 8760 ساعة منذ صدور العدد الأول من "مجلة سيكيورتي كايزن" (Security Kaizen). ونحتفل معكم اليوم بعيد مولد المجلة الأول.

فقد مرت الأيام سريعًا وأعتقد أننا جميعًا نشعر بالشعور ذاته، فلا زلت أتذكر حتي الآن كما لو كان الأمر حدث الشهر الماضي على الرغم من مرور عامًا كاملاً على أيام ثورة الخامس والعشرون من يناير وميدان التحرير وقطع الإنترنت والاستيقاظ طوال الليل لحراسة المنازل.

خلال هذا العام، إذاكان لدي الحق في قول ذلك، فقد كنا ننتقل من نجاح إلى آخر، وردود الفعل التي وصلتنا من مُتابيعنا سواءًا على المستوى العالمي أو المحلي كانت أكثر وأبعد مما توقعت وجعلتني أشعر بفخر شديد - ليس فخرًا بنفسي أكثر مما هو فخرًا بما قام به فريقي على الرغم من الظروف الصعبة التي مرت بها البلاد، فقد كنا قادرين على الاستمرار وعلى تحسين عملنا.

2011 ACHIEVEMENTS

لقد تلقينا العديد من الطلبات لإصدار المجلة باللغة العربية بعد إصدار العدد الأول من المجلة باللغة الإنجليزية، ولذا فقد بدأنا بالعمل على ذلك وبدأنا بإصدار المجلة بالغتين الإنجليزية والعربية بدءًا من العدد الثاني وقد كان من الصعب ترجمة بعض المصطلحات والمفاهيم التقنية إلى اللغة العربية خاصةً وأن مُترجمينا لم يكونوا متخصصين في المجال التقني ولذا أنا أُحب أن أغتنم الفرصة لشُكر جميع المترجمين الذين قاموا بمساعدتنا في إصدار الأعداد العربية حتى وصلنا إلى مستوى ثابت.

وقد كنا قادرين على أن نكون الراعي الإعلامي لمعظم مؤتمرات أمن المعلومات الشهيرة خلال عام 2011 بدءًا من مؤتمر Hacker Halted الذي أقيم في القاهرة في ديسمبر 2010 ومرورًا بمؤتمر HITB الذي أقيم في أمستردام وماليزيا، ومؤتمر Takedowncon الذي أقيم في دالاس، ومؤتمر Hacker Halted الذي أقيم في ميامي، ومؤتمر RSA الذي أقيم في لندن، ومؤتمر Cyber Defense Summit الذي أقيم في أبو ظبي ومؤتمرات أخرى. وقد كنا الراعي الإعلامي أيضًا لأول ألعاب الأولمبياد العالمي للأمن الإلكتروني (Cyberlympics).

وأكثر ما أدهشني هو أنه على الرغم من غلاء ثمن تذاكر هذه المؤتمرات –فقد كان متوسط ثمن التذكرة يصل إلى 2000 $ - إلا أن قُرائنا من الولايات المتحدة وأمستردام ولندن كانوا حريصين كل الحرص على حضور المؤتمرات باستخدام رمز الخصم الخاص بنا. فقد كنا قادرين على جعل قارئ واحد في أمريكا القيام بحضور مؤتمر Takedowncon في دالاس و4 قُراء في أمستردام لحضور مؤتمر HITB وقارئ واحد لحضور مؤتمر RSA في لندن.

وقد قمنا بإجراء مقابلات مع مختصين مرموقين في مجال أمن المعلومات مثل: جو سوليفان (رئيس قسم أمن المعلومات في موقع فيس بوك). ولقد كنا قادرين أيضًا على إجراء شراكة مع موقع الفيس بوك حيث سيقوم فريق مُتخصص بكتابة مقال في كل عدد حول التلميحات الأمنية في موقع الفيس بوك (Facebook.com). وقد قمنا بإجراء مقابلة مع كليمنت دوبوي (مؤسس بوابة CCCURE.ORG) ومع آل برمان (الرئيس التنفيذي لـ DRII.ORG) وفي هذا العدد قمنا بإجراء مقابلة مع د\ شريف هاشم، كبير مُستشاري وزير الاتصالات وتكنولوجيا المعلومات للأمن الإلكتروني، ونائب الرئيس التنفيذي لهيئة تطوير صناعة تكنولوجيا المعلومات (ITIDA)، بمصر.

التحديات

إن أكبر التحديات التي واجهتنا خلال هذا العام كانت في تحويل المجلة من نسخة إلكترونية إلى نسخة مطبوعة، فطباعة المجلات ليست رخيصة خصوصًا أن «مجلة سيكيورتي كايزن» مجلة مجانية والمصدر الوحيد لتغطية المصاريف هو من خلال الإعلانات وكلنا نعلم مدى صعوبة العمل خلال هذا العام والذي تسبب في إغلاق بعض الشركات، ولكننا كنا قادرين على القيام بذلك وعلى الاستمرار في القيام بذلك.

وبسبب هذه المشاكل المادية، لم نكن قادرين على إصدار العدد الرابع في موعده وكان علينا القيام بدمج عدد شهر أكتوبر مع عدد شهر يناير معًا ليتم إصدارهم في عدد واحد في شهر ديسمبر ليكون عدد سنوي، ولكننا حاولنا أن نجعل هذا العدد مُختلفًا ومُميزًا وأتمنى أن يحوز إعجابكم. ولكن لنكون قادرين على مواصلة إصدار المجلة وإبقاءها مجانية، فقد قررنا القيام بالحصول بنوع من التمويل من جميع مُحبي

مُنظمة «بلو كايزن» و«مجلة سيكيورتي كايزن» الذين توجد لديهم اللاغبة في مشاركتنا، وعادةً في مثل تلك الحالات في البلاد الغربية يكفي وجود «زر للتبرع» في موقع الويب، ولكن لا تتوفر لدينا هذه الثقافة في دول الشرق الأوسط ولذا فقد قررنا إنشاء قسم تحت اسم «سوق بلو كايزن» وسوف تتمكن من خلال هذا القسم القيام بشراء مُنتجات بول كايزن المُختلفة مثل: الأكواب والقمصان التي يوجد عليها شعار (سيكسورتي كايزن)، ورسوم الشخصية المُتحركة «كايزونو» والعديد من الأشكال الأخرى. لقد كنا نُفكر في فكرة كي لا تُعد كنوع من أنواع التبرع المالي المُباشر وقد وجدنا أن هذا الحل هو الأفضل. ولذا إذا كنت من مُحبي مجلتنا وأنشطتنا، فساعدنا على مواصلة إصدارها عبر مساهمتك في فكرة «سوق بلو كايزن».

وأخيرًا، أنا لا أقول هذا لأفتخر بما قمنا بفعله، على الرغم من وجوب ذلك، ولكن لمشاركة هذا النجاح مع قُراءنا الأعزاء ولتأكيد أننا لم نكن لنصل إلى هذا النجاح بدونهم. وأيضًا لشُكر أعضاء فريقي الذين تطوعوا بوقتتهم ومجهودهم لأنهم آمنوا بأهداف «بلو كايزن» وأُريد أن أُخص بالشكر «مريم سامي» (مُطورة ومُصممة موقعنا)، و«مي علاء» وفريقها (مُترجمتنا) الذين قاموا بمجهود كبير خلال هذا العام لدفع «سيكيورتي كايزن» إلى الأمام وأخيرًا أحب أن أشكر زوجتي كثيرًا التي لولا مُساندتها لي وتوفيرها للمناخ الملائم لم أكن لأصل إلى هذا النجاح.

Moataz Salah
Bluekaizen founder

orange™

Together, we can do more

Security Solutions Engineer- Proxy & Cashe

(Ref: 526460)

- Very good understanding of networking (TCP/IP, routing OSPF, switching)
- Very good understanding of application & network security concepts & technologies
- In depth experience of Bluecoat proxies and preferably BCCPA & BCCPP certified.
- Good knowledge of Bluecoat (or else) reporting systems (Reporter), management systems (Director),
- content delivery network (CDN), data leakage prevention (DLP) and cloud computing.
- Sound understanding of service design especially validation, testing and release management.
- Hands- on experience in analyzing architecture and building proposals.
- Ability to write technical documentation for operations, sales and marketing.
  working knowledge routing, load balancing and resiliency.

Security Solutions Engineer- Intrusion Detection

(Ref: 526461)

- Very good understanding of networking (TCP/IP, routing OSPF, switching)
- Very good understanding of application & network security concepts & technologies
- In depth experience of Juniper IDP sensors and preferably JNCIA -IDP certified.
- Good Knowledge of security event & incident management systems (Archsight) and working experience in developing signature and tuning sensors as well as investigating security incidenta.
- Sound understanding of service design especially validation, testing and release management.
- Hands- on experience in analyzing architecture and building proposals.
- Ability to write technical documentation for operations, sales and marketing.
- working knowledge routing, load balancing and resiliency.

Mobility Operation Engineer

(Ref: 525906)

- Working experience in routing and VPN configuration.
- Very good understanding of traffic security technologies and products in particular IPSec using Nortel
- Contivity & SSL using Juniper SSL-VPN; JNCIA-SSL is a plus.
- Working experience in authentication systems and in particular in RADIUS, TACACS, AAA & PKIs.
- Very good understanding of host firewalls Antivirus and HIPS notably from BigFix.
- Excellent understanding of IT & networking fundamentals.
- Good understanding of remote access technologies and mobility technologies.
- Good understanding of Unix/ Linux and certification is a plus.
- Good understanding of ITIL incident & change management processes.

Internal Security Engineer

(Ref: 527064)

- Very good understanding of information security concepts and mainly access control domain.
- Very good understanding of networking (TCP/IP, routing OSPF, switching)
- Working experience in administration and management of firewalls & proxies (as security not acceleration devices) notably Checkpoint FWs & Bluecoat proxies.
- Knowledge and practice of Windows & Unix systems administration required
- Knowledge of security technologies such as Authentication, Encryption, PKI, Anti- Virus, Firewalls and Intrusion protection.
- Practice of network and security support & operations appreciated.
- Certification in security products is a plus.
- Very good understanding of ITIL processes and mainly change management process.

Chek the jobs in http://jobs.orange.com
Or email osama.hijji@orange.com

True STORY

اختراق البنوك من أجل المتعة والربح

"You know, you can do this just as easily online."

الخداع والخيانة والسرقة هي أشياء معروفة للإنسان منذ العصر الحجري. والتاريخ هو الشاهد علي العديد من أعمال الخداع التي قام بها الإنسان لاستغلال وخداع وسرقة الأبرياء. حاليًا ومع تحول العالم لشكل جديد يُحركه التقدم التكنولوجي، تبقي طباع الإنسان كما هي. وقد أدى هذا التقدم الي تنوع أساليب النصب عن العصور السابقة. والآن يتم كثيرًا إساءة استخدام الإنترنت لارتكاب الجرائم في الفضاء الالكتروني. وتُعد جرائم "اختراق البنوك" هي الجرائم التي يتم ارتكابها بكثرة بين مُجرمي الإنترنت وبين الجرائم الأخرى التي يتم ارتكابها في الفضاء الإلكتروني.

لنلقي نظرة علي عمليات السطو علي البنوك عبر الإنترنت التي حدثت خلال السنتين الماضيتين:

• في منتصف يوليو2010 قام مُحتالوا الكمبيوتر بسرقة مبلغ 447000 دولار من شركة Ferma Corp. في سانتا ماريا- كاليفورنيا والتي تقع في شركة Demolition Company عن طريق نقل دفعات كبيرة من التحويلات من حساب شركة Ferma المصرفي علي الإنترنت.

• وأيضًا في يوليو 2010 قام المهاجمون بسرقة مبلغ 415000 دولار من بنك Bullitt County في ولاية كنتاكي بالولايات المتحدة.

• وفي ديسمبر 2009 نجح مُجرمي الفضاء الإلكتروني في سرقة 300000 يورو من الحسابات المصرفية علي الإنترنت للبنوك الألمانية.

• وتطول القائمة...

• وتتطور طرق عمل مُجرمي الفضاء الإلكتروني باستمرار لسرقة واختراق البنوك لتواكب التكنولوجيا الحديثة التي يتم استخدامها في البنوك.

خطة الهجوم الأساسية:

لكي ينجح الهجوم، يجب أن يقوم المُهاجم أولاً بالتحكم عن بُعد بجهاز كمبيوتر أحد مُستخدمين البنك المُتصلين بالإنترنت والذي من خلاله يقوم المُستخدم بعمل حوالات بنكية. وعلى الرغم من وجود الكثير من الطرق للتحكم عن بُعد بجهاز الضحية فإن أسهل الطرق هي مهاجمة تطبيقات سطح المكتب مثل متصفح الإنترنت أو تطبيق PDF reader أو تطبيق MS-Office و غيرهم من التطبيقات التي يتم تحميلها بشكل افتراضي علي جهاز الضحية. تحتوي هذه التطبيقات علي العديد من الثغرات ونقاط الضعف التي يُمكن للمُهاجم اختراقها عن بُعد لتعطيهم وصول غير مُصرح به لجهاز الضحية.

ومن الممكن أن تتم مهاجمة هذه التطبيقات تتم بأكثر من طريقة. وأسهل هذه الطرق هي عبر إرسال بريد إلكتروني مُخادع لمُستخدم البنك والذي يحتوي على مُرفق PDF أو MS-officeمع برنامج مُخبأ داخل المُرفق. يُعد هذا البرنامج نوعًا من برامج سرقة البيانات (Trojan horse) وقد يظهر البرنامج كملف غير مؤذي ولكن وظيفته الأساسية هي توصيل جهاز الضحية بخادم يقوم المُهاجم بالتحكم به.

وبدلاً من أن يقوم المُهاجم بإرسال بريد إلكتروني مُباشر، فسوف يحاول جذب المُستخدم لزيارة مواقع إلكترونية احتيالية

يتحكم بها المُهاجم والتي تحتوي علي شفرة هجوم مخفية بداخل الموقع. وبمجرد دخول المُستخدم على تلك المواقع يتم مهاجمة متصفح الإنترنت الخاص به تلقائيًا وإجبار جهاز الكمبيوتر الخاص بالمُستخدم على تنزيل برامج تروجان (Trojan) ضارة بدون علم المُستخدم.

برامج تروجان (Trojan) ضارة للبنوك:

يقوم مُجرمي الإنترنت باستخدام برامج تروجان (Trojan) المصرفية مثل: "Zeus" و"LuckySpoilt" و"MPack" و"Clampi" و"URLZone" وغيرهم من برامج التروجان المُخصصة لهذه الأهداف. بعض برامج التروجان هذه مُتاحة تُجاريًا للبيع بسعر بسيط مثل 500 دولار مع إمكانية الحصول علي التحديثات والدعم عن بُعد والصيانة السنوية وأشياء أخرى.

تكون برامج التروجان (Trojan) هذه مُصممة خصيصًا لاختراق حسابات البنوك على الإنترنت ويأتي معها جميع الإمكانيات التي تُسهل عملية اختراق البنوك للمهاجمين. ومن الخصائص التي نجدها في بعض الفيروسات مثل URLZone أو Zeus:

- إمكانية الوصول إلى أوراق الاعتماد وحسابات البنوك الجارية.
- إمكانية أخذ صور من الصفحات التي تُقدمها المواقع.
- إمكانية سرقة النقود من حسابات التسوية.
- إمكانية إخفاء التحويلات الاحتيالية من تقرير حسابات التسوية.
- إمكانيه إرسال تعليمات لبرامج التروجان من الخادم الخاص بالمُهاجم عن كمية النقود التي تريد سرقتها والحساب الذي سيتم التحويل إليه.
- معرفة السجلات والتقارير عن حسابات لإلإنترنت الأخرى مثل : (Facebook و-Pay Pal وGmail) والبنوك من بلاد أخرى.

وتُباع النُسخ الحالية من ZeuS بحوالي 10000 دولار وتُستخدم بواسطة نُخبة من عصابات الإنترنت لتحويل الأموال من الحسابات المصرفية للشركات الصغيرة ومتوسطة الحجم على الإنترنت.

تم إطلاق نوعًا جديدًا من برامج التروجان والذي يُسمى بـ «OddJob» والذي يستهدف الحسابات البنكية ويقوم بالوصول غير المُصرح إلى المعلومات (Session Hijack-ing) الخاصة بحساب الهدف باستخدام مُعرف القسم (session ID) الخاص به. تقوم برامج التروجان هذه بإبقاء حسابات المُستخدم مفتوحة حتى بعد أن يعتقد المُستخدم أنه قد قام بتسجيل الخروج منها مما يُمكن المُهاجم من القيام بعمليات النصب وتحويل الأموال بشكل غير ملحوظ. ويقوم هذا النوع الجديد من البرامج الضارة بدفع وتطوير طرق الاختراق من خلال تطور منهجية الهجوم الحالية. وهذا يدل على مدى براعة المُهاجم والتي تُمكنه من تجنّب تطبيقات أمن تكنولوجيا المعلومات التُجارية والتي يتم استخدامها بشكل تقليدي لحماية حسابات المصرفية الخاصة بهم عبر الإنترنت.

وحتي وقت كتابة هذه السطور ظهر رروجان مصرفي أكثر خطورة باسم «tatan-ga.» ويستطيع تروجان «tatanga» اختراق متصفح الإنترنت explorer.exe ويُمكن أن يقوم بإدخال HTML في جميع متُصفحات لإلإنترنت مثل: Internet Explorer و-Moz illa Firefox وGoogle Chrome وOpera و (Minefield (Firefox dev builds و-Maxt hoon وNetscape وSafari وKonqueror.

كيف يعمل التروجان المصرفي؟

يظل التروجان مُختبئًا في متصفح المُستخدم وينتظر حتي يقوم المُستخدم بتسجيل الدخول إلى الموقع الخاص بالبنك. أثناء عملية تسجيل الدخول يقوم التروجان بنسخ اسم المُستخدم وكلمة المرور ويقوم بإرسالها إلى المُهاجم ثم يمنع المُتصفح من إرسال طلب تسجيل الدخول إلى الموقع

الخاص بالبنك ويقوم بإخطار المُستخدم أن «الخدمة غير مُتاحة مؤقتًا.» ومن ثَّم يستخدم السارق اسم المُستخدم وكلمة المرور لتسجيل الدخول إلى الحساب المصرفي وسرقة كل مافيه من نقود.

تقوم بعض أنواع التروجان بإعادة كتابة المُعاملات المُرسلة بواسطة المُستخدم إلى الموقع المصرفي عبر الإنترنت وتملأها بالمُعاملات الخاصة بالسارق. وتحدُث عملية إعادة الكتابة هذه بدون علم المُستخدم حتى أن المُستخدم لا يرى قيم المُعاملات التي تمت مراجعتها. وبالمثل، ستقوم العديد من البنوك المصرفية عبر الإنترنت بالتواصل مرة أخرى مع مُتصفح المُستخدم وإرسال تفاصيل المُعاملات التي تحتاج إلى تأكيد المُستخدم باستخدام إدخال كلمة مرور المرة الواحدة، ولكن البرنامج الضار يقوم بتغيير القيم التي يراها المُستخدم مرة أخرة إلى القيم التي قام المُستخدم بإدخالها في البداية. وبهذه الطريقة لا يكتشف المُستخدم أو البنك أنه قد تم تغيير البيانات التي تم إرسالها.

أما المُعاملات التي تعتمد على المكالمات التليفونية للموافقة على إجراء المُعاملات فيقوم فيها الشخص المُحتال باستخدام طريقة بسيطة وهي أن يطلُب من المُتصل تحويل المكالمة من رقم المُستخدم إلى رقمه الخاص لصعوبة الوصول للرقم الأصلي ويقوم المُتصل بتحويل المكالمة دون التأكد من هوية المُتحدث قبل تنفيذ الطلب.

مركز خدمة الأوامر والتحكم

بعد إصابة جهاز الضحية، يقوم التروجان بالاتصال بمراكز خدمة الأوامر والتحكم لتلقي التعليمات. وعادةً ما تكون مراكز الخدمة هذه في روسيا وبلاد الشرق أوروبية البعيدة. وعندها يقوم مركز خدمة الأوامر والتحكم بإرسال التعليمات التي تحتوي على كمية النقود المطلوب سرقتها ورقم حساب السارق لتحويل النقود إليه وأيضًا الحصول على صورة خاصة بالواجهة المصرفية عبر الإنترنت، وغيرها.

مُحولي الأموال المسروقة

ويقول الخبراء القانونيين أن مُحولي الأموال المسروقة هم عادةً أشخاص راغبون أو غير مشكوك بهم ويتم توظيفهم عبر الإنترنت تحت مُسمى «وكيل محلي» أو «وكيل مالي» ليكون مسئولاً عن نقل الأموال باسم شركة دولية، وبمجرد أن تقوم عصابات الإنترنت بتوظيف المُحول بتحويل الأموال المسروقة إلى حساب المُحول المصرفي ثم يطلب منه أن يقوم بتحويل الأموال بعد أن يأخذ عمولته إلى الحساب المصرفي الذي يُخبره به العصابة عبر البريد السريع إلى الدول الشرق أوروبية بعيدة.

تفادي أنظمة مكافحة الاحتيال

لتفادي إشارات الإنذار من أنظمة مكافحة الاحتيال في البنوك فيتم استخدام حسابات المُحول لعدد محدود من المرات لفترة زمنية مُحددة. وحيث أن البنوك تقوم بمُراقبة عمليات تحويل الأموال الكبيرة فيجب أن يتم إيداع كمية أموال صغيرة لتُبقي العملية غير مُراقبة.

وللحد من فُرص الكشف من قِبل أنظمة مكافحة الاحتيال، يقوم مُجرمي الإنترنت باستخدام الكثير من المعايير لتحديد كمية النقود التي سيقومون بسرقتها في كل مرة، ومن ضمن هذه المعايير: التأكد أن رصيد الضحية كافي، والتأكد أن كمية الأموال المسروقة ليست كبيرة، ونقل كمية عشوائية مختلفة من الأموال كل مرة، والتأكد أنه سيتبقى رصيد في الحساب بعد التحويل.

كيفية تجنُب الاكتشاف من قِبل الضحية

وحتى يستمر المُحتال في أعماله السيئة بسرية، يحتاج مُجرمي الإنترنت إلى إخفاء عمليات تحويل الأموال غير القانونية عن الضحية، وإلا فسيخسرون إذا اكتشفت

الضحية أين يتم تحويل الأموال وقام بإبلاغ البنك عنها. ولتقليل فرصة اكتشافهم يقوم التروجان بإنشاء صفحة تقرير بنك مزورة لتقديمها للضحية ويخفي المُعاملات المسروقة من جهاز الضحية ثم يقوم بإرسال التقرير إلى جهاز المُصاب.

وفي حالة البنك الألماني التي اكتشفتها مجموعة الأمن M86 ظهرت كمية النقود المُحولة 53.94 يورو بدلاً من القيمة الحقيقة والتي تبلُغ 8576.31 يورو. قام التروجان بإنشاء صورة مزورة لإظهار قيمة التحويل 53.94 يورو وإرسالها إلى مركز الخدمة الأوامر والتحكم كصورة. وإذا قام الضحية بتسجيل الدخول إلى حسابه المصرفي من جهاز كمبيوتر آخر غير مُصاب بالتروجان تظهر له قيمة التحويل الحقيقية.

الاستنتاج:

أصبحت الهجمات والمُهاجمين الإلكترونيين أكثر تعقيدًا بكثير ولابد من ضرورة حماية أموالنا وموارنا من تلك الأخطار.

يجب أن يتم تنبيه مُستخدمي البنوك عبر الإنترنت بتطورات الطرق المُختلفة التي يستخدمها مُجرمي الإنترنت. ويجب أيضًا أن يتأكد المُستخدمين من نُظم الحماية في أجهزتهم عن طريق تحميل أدوات الأمان التي ستُنبههم في حالة وجود أي نشاط مُريب.

يجب أن تستخدم البنوك والمؤسسات المالية حلول أمان مُوحدة للإنترنت مثل تطبيقات حماية الإنترنت التي تقوم بفحص المحتوى في الوقت الحقيقي لتحسين الحماية وتوثيق مُتعدد المستويات وغيرهم. ينبغي أن تضع البنوك استخدام المقاييس الآتية في الحسبان:

- مركز خدمة كشف الاحتيال لمراقبة المُعاملات المشكوك فيها.
- التحقق من المُعاملات غير المُعتادة لتأكيد طلب المستخدم وتنفيذ المُعاملات المؤكدة أو المُوقعة من المُستخدم.
- وجود قوانين اتصالات يُمكنها منع تحويل المكالمات إلى أرقام لم يتم تسجيلها في مستخدم حساب مُحدد

هداية الله خان

الرئيس التنفيذي لشركة استشارية في تكنولوجيا المعلومات تُدعى Sentelist Middle East مُتخصصة في تطبيقات الأمان واختبار الاختراقات والتحقيق فيها

Security Kaizen Labs 2012

Registration Opening Soon

It's time

To learn how hackers do it

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

2day adv.

Cracking into a Wireless Network or Make a Sandwich?

هذا صحيح، فلقد بدأ الأمر بينما كنت جائعًا جدًا وأحاول اكتشاف ما الذي يُمكنني تناوله أثناء زيارتي الأخيرة لعائلتي وقد اكتشفت أن أخي قد قام بتغيير كلمة مرور الاتصال اللاسلكي.

وفي اللحظة التي بدأت فيها بالتفكير فيما يُمكنني القيام به قفز إلى عقلي أسماء بعض التطبيقات مثل aircrack-ng أو weplap أو WEPCrack أو airsnort. وفيما أمعنت النظر في الغرفة من حولي في محاولة التحقق مما يُمكن أن يكون قد تغير أيضًا، وجدت قرص مدمج صغير مُؤسس على نظام التشغيل المُصغر Tiny Core Linux المُسمى "Beini" من نظام التشغيل الحُر GNU/Linux ذو التوزيع الصيني والذي تم إنشاؤه وصيانته بواسطة تشاو تشون شنج (Zhao Chunsheng) من تيانجين، الصين على مكتبي.

إن هذا التوزيع غير معروف و\أو غير مُستخدم بشكل شائع، ومع ذلك فهو خفيف جدًا وإذا كنت ترغب في طريقة سهلة وبسيطة للوصول إلى شبكة لاسلكية، فإن "Beini" هو أفضل أداة مصدر مفتوح للقيام بذلك.

فقد استغرق الأمر أقل من دقيقة لتشغيل القرص المُدمج وبضع دقائق أخرى للحصول على مفتاح الوصول إلى الشبكة اللاسلكية المنزلية.

وأنا على وشك أن أُبين كيفية الوصول إلى إحدى الشبكات اللاسلكية خطوة بخطوة، أولاً دعوني أبين كيف أفكر وما هي التقنيات التي يُمكن استخدامها في الشكل الموضح أدناه (الشكل 1):

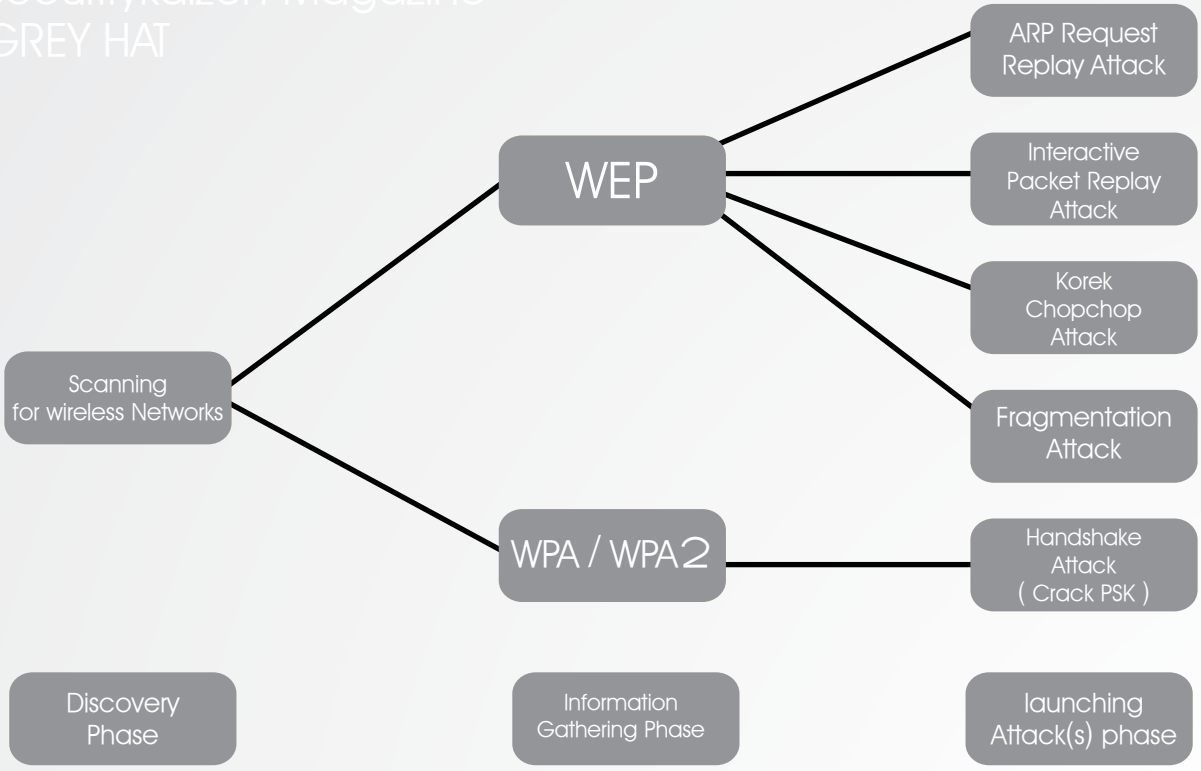


Figure 1. Wireless/Security Cracking Techniques

بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP)

على الأرجح قد أقوم باستخدام تقنيات الوصول التالية:

1. طلب إعادة الهجوم ARP

هذه الطريقة فعالة جدًا لإنشاء ناقلات تهيئة جديدة (IV)، يقوم البرنامج بالاستماع إلى إحدى حِزم بروتوكولات إيجاد العنوان (ARP) ثم يقوم يقوم بإعادة بثه إلى نقطة الوصول. تستمر نقطة الوصول في الاستجابة إلى بروتوكولات إيجاد العنوان (ARP) (ناقلات التهيئة الجديدة (IV)) ومن خلال هذه الطريقة سنكون قادرين على تحديد مفتاح بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP)

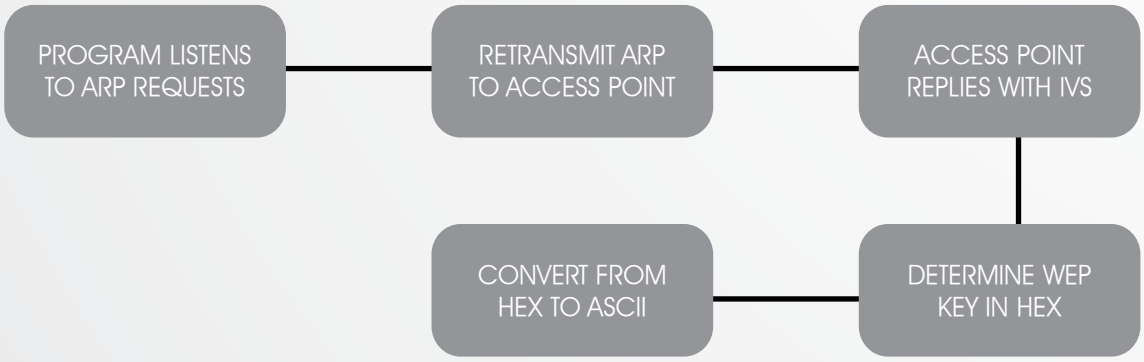
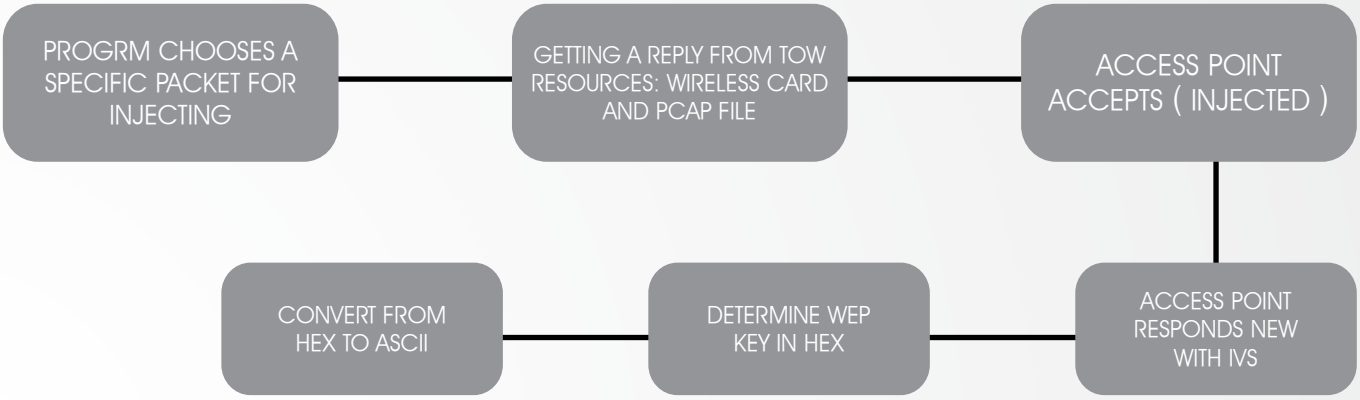


Figure 2. ARP Request Replay Attack Process Flow

2. حزمة إعادة الهجوم التفاعلية

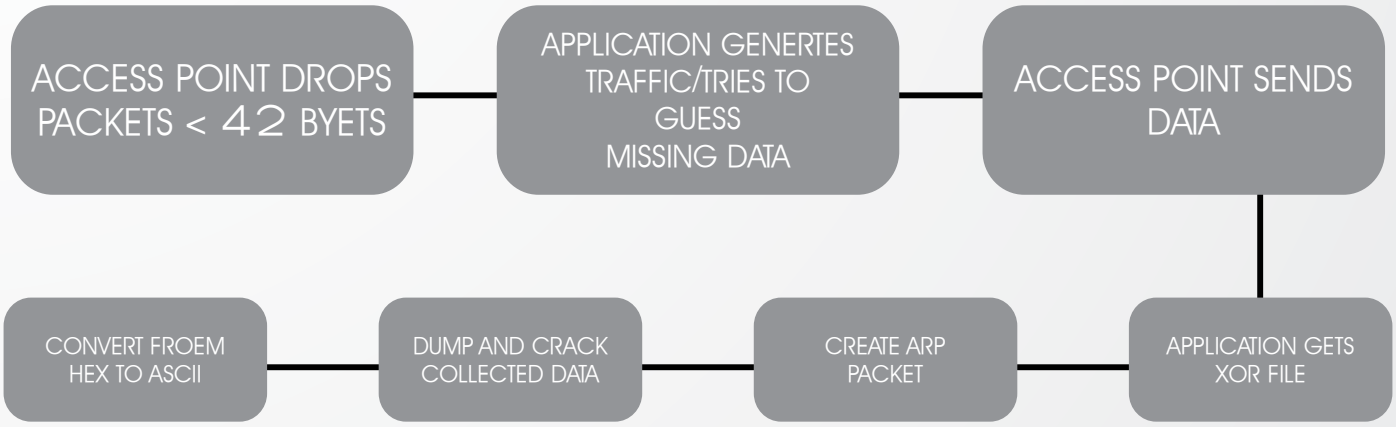
تتيح لك هذه الهجمات بحقن الحِزم والحصول عليها لإعادة تشغيلها من البطاقة اللاسلكية الخاصة بك وملف pcap (هل سمعت عن ملف يُسمى "libpcap" من قبل؟ ربما؟). قد تعمل بعض الحِزم فقط (ليتم قبولها من قِبل نقطة الوصول) والتي تتسبب بدورها في ناقلات التهيئة الجديدة (IV)، وهذا هو الهدف من هذه العملية بالكامل، ناقلات تهيئة جديدة (IV) لإيجاد مفتاح بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP).



الشكل 2. تدفق عملية طلب إعادة الهجوم ARP

3. هجوم KoreK ChopChop Attack

فك تشفير حزمة واحدة! الكشف عن النص العادي. يُمكن للهجمات الناجحة أن تقوم بفك شفرة حزمة بيانات بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP) بدون الحاجة إلى معرفة المفتاح. ومن الجدير بالذِكر أيضًا أنه من الممكن أن تعمل هذه الهجمات ضد آليات بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP) والذي يُعد مجموعة من تقنية 802.1x وبروتوكول (Extensible Authentication Protocol - EAP) -- تقوم آلية بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP) بتغيير مفاتيح بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP) بشكل آلي.



الشكل 3. تدفق عملية حزمة إعادة الهجوم التفاعلية

4. هجوم Fragmentation Attack

مرة أخرى، لا يقوم هجوم Fragmentation Attack باسترداد مفتاح بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP) بنفسه، ولكن يُمكنه فقط الحصول على مرحلة توليد القيم شبه العشوائية (Pseudo Random Generation Algorithm - PRGA). يُمكن استخدام مرحلة PRGA لاحقًا لإنتاج الحِزَم والتي في المقابل تقوم بالمساعدة في حقن الهجمات أيضًا. يحصُل الهجوم على طول الحزمة بالكامل وهو 1500 بايت xor، ولذا يُمكن إنتاج أي حجم من الحِزَم وهو كافٍ لإنشاء طلب ARP.

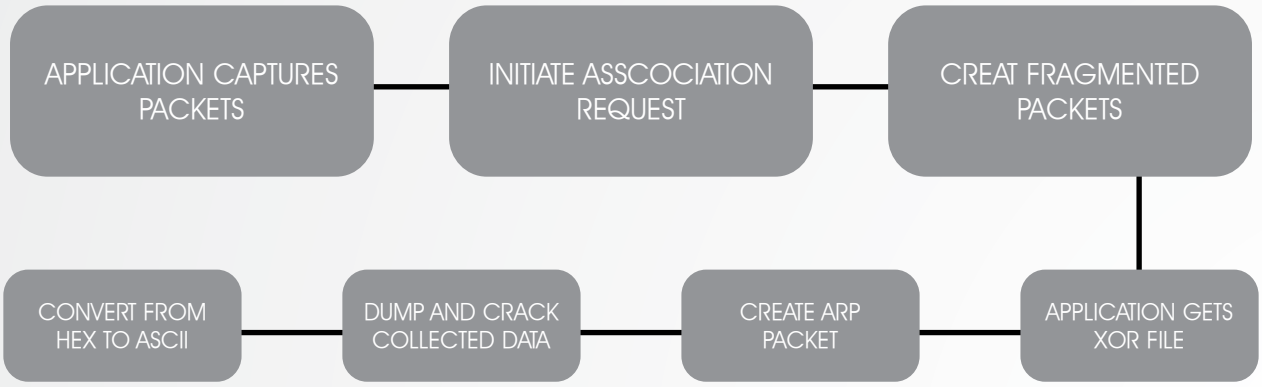


Figure 5. Fragmentation Attack Process Flow

بروتوكول وصول Wi-Fi المحمي (WPA/WPA2)

يُعد نظام المصادقة هو ذاته في الاثنين، يجب أن يتم نشر هجوم Dictionary Attack وإلا بخلاف ذلك فلا تُفكر في الأمر (في حالة القوة المفرطة\فشل هجوم Dictionary Attack)

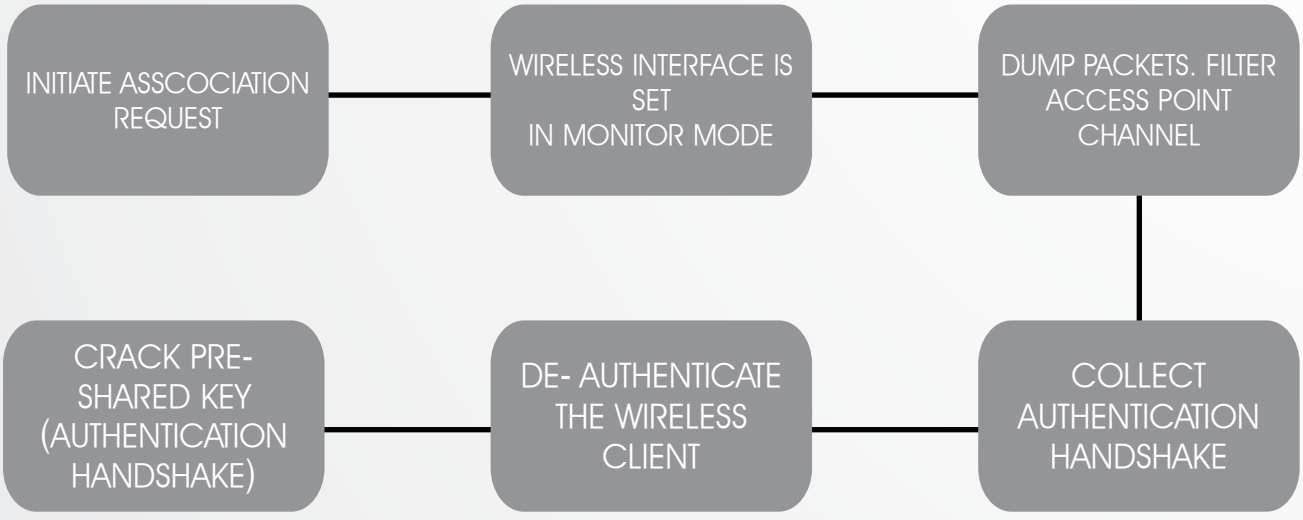


Figure 6. WPA/WPA2 Attack(s) Process Flow

حسنًا حسنًا،
كفانا حديثًا، هيا بنا لنبدأ باختراق بعض الشبكات.

أولاً، سأقوم بتشغيل جهازي باستخدام قرص Beini المُدمج (من خلال وصلة USB stick أو من خلال إحدى الأقراص المُدمجة العادية)

Figure 7.

First Screen After Booting Beini Live-CD

قم باختيار رمز "FeedingBottle" (زجاجة التغذية) من شريط المهام.

Figure8.

Launching "Feeding Bottle" Application

يُرجى تَذكُر، أن هذا مجرد إثبات للمبدأ ويُمكنك تجربته على نقطة الوصول الخاصة بك فقط.

بعد النقر فوق "نعم" سترى الشاشة التالية لتمُكنك من اختيار البطاقة اللاسلكية الخاصة بك ثم قم بضبط الوضع على وضع "مراقبة".

Figure 9.

Choosing Wireless Card (Monitor Mode)

وبمجرد أن تقوم بالنقر فوق "التالي ->" ثم "مسح" ويبدأ برنامج airdump-ng بالتقاط إطارات 802.11 الأولية ليبدأ بتجميع ناقلات التهيئة (IV).

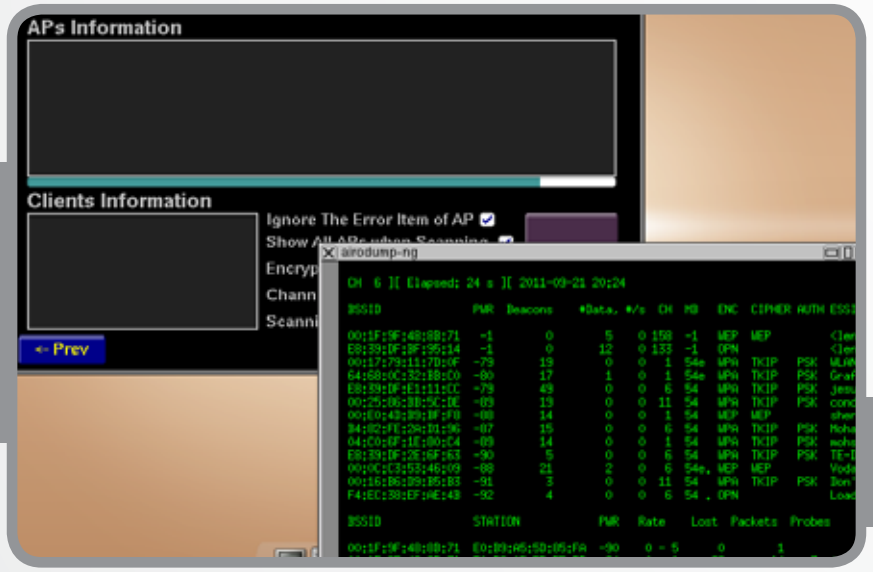


Figure 10.

Airdump-ng Capturing

بعد مسح الشبكة الكبيرة (تجود العديد من الشبكات لاختراقها) أقوم باختيار نقطة الوصول الخاصة بمنزلي فأنا شاب طيب.

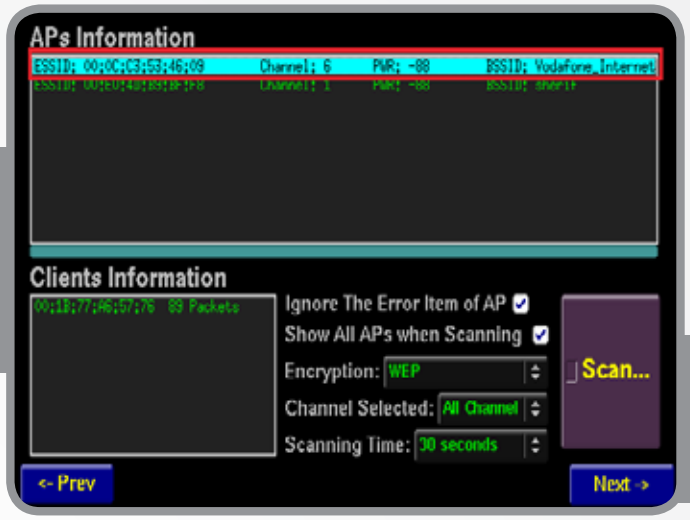


Figure 11.

WEP Wireless Access Point Found

وكما ذكرت سابقًا، فإنني أُفكر في أربعة هجمات لإطلاقهم ضد بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP) والتي من خلالها يُعد "طلب إعادة الهجوم ARP" الأسرع ويُعد "هجوم Fragmentation Attack" الأطول، وأكثر موثوقية على الأقل من وجهة نظري بما أن "هجوم Chop-Chop Attack" لا يعمل مع جميع نقاط الوصول. وفي إثبات المفهوم هذا سأعرض لكم الطريقة الأطول وهي "هجوم Fragmentation Attack".

بمجرد أن يتم إطلاق الهجوم، سيقوم برنامج airdump-ng بالالتقاط، وتُعد ناقلات التهيئة (IV) مفتاح نجاحنا، سنحاول بدء ربط طلب المصادقة الوهمي.

Figure 12.

Launching Fragmentation Attack

الآن يحدث الربط، وسيتم إرسال الحِزَم المُجزئة وإنتاج مفتاح ملف التدفيق (سيُساعد ملف xor في إنشاء الحِزَم بدون معرفة المفتاح).

بعد الحقن، يتم التقاط ناقلات التهيئة (IV) وتجميعها لبدء اختراق الشبكة. إن التقاط\تجميع ناقلات التهيئة (IV) هو ما يهم وليس الحِزَم لأنها لا تساعدنا في اختراق بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP) وستكون العديد من الحِزَم إرشادية (حيث يتم بثها بواسطة نقاط الوصول لإظهار وجودهم - هاي أنا هنا!).

عندما يتم التقاط عدد كافي من ناقلات التهيئة (اعتمادًا على حجم مفتاح بروتوكول الخصوصية

Figure 13.

Generating XOR File, Forged ARP Request and Injecting

على قنوات الاتصال اللاسلكية (WEP)) ستجد أن برنامج الاختراق قد بدأ في العمل بسهولة وبعد بضعة دقائق ستظهر لك رسالة "تم العثور على المفتاح". سترى أدناه أنه قد تم العثور على المفتاح وستجده أيضًا مُحَولاً إلى أسكي (ASCII) من هيكس (HEX).

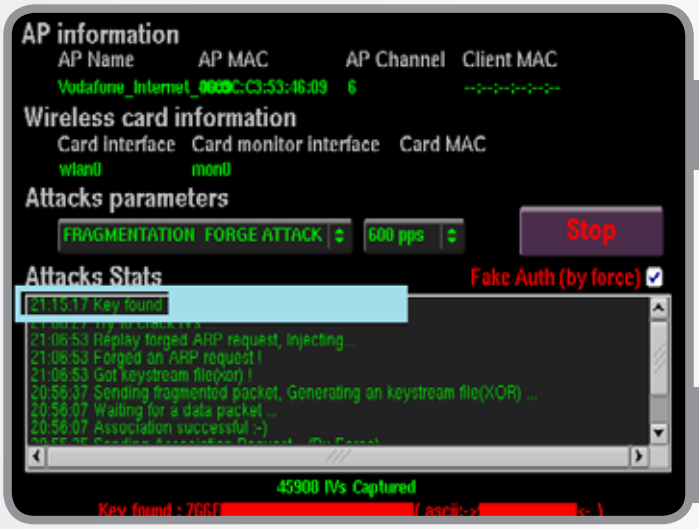


Figure 14.

Cracking IVs, Key Found

وأخيرًا، يُمكن أن يكون اختراق الشبكات اللاسلكية أمرًا سهلاً، ومن المُمكن أن يأخذ بضع دقائق، خصوصًا في حالة أمن بروتوكول الخصوصية على قنوات الاتصال اللاسلكية (WEP). وفي هذه الحالة، من المُوصى به بشدة تشغيل وضع الأمن الأحدث WPA2 والذي يقوم باستخدام المعيار المتقدم للتشفير (AES) ويستخدم تقنيات أمنية أعلى من أجل حماية الشبكة اللاسلكية الخاصة بك. ومن الجدير بالذِكر أيضًا أن قوة كلمة المرور الخاصة بك تلعب دورًا رئيسيًا، لذا يُرجى وضع استخدام كلمة مرور قوية في الاعتبار بما في ذلك استخدام أحرُف كبيرة وأحرُف صغيرة وأرقام ورموز. وأخيرًا وليس آخرًا، يُرجى استخدام المعلومات الواردة أعلاه بحكمة، ويُرجى تذَكُر: "تأتي المسؤولية العُظمى مع القوة العُظمى" - سبايدر مان.

Sameh Sabry

I am Security Consultant, OSCP, LPT, CHFI, C|EH, SANS PCI/DSS, Security+, Linux+, RHCE, LPI, CCNA

CSRF موضوع

ما هو هجوم CSRF؟

يُعد تزوير الطلبات عبر المواقع (CSRF – Cross-Site Request Forgery) نقطة ضعف في تطبيقات الويب. فهو يُمَكّن المهاجم من الحصول على أي نوع من المعلومات من خلال إنشاء موقع إلكتروني أو بريد إلكتروني بعد أن يقوم المُستخدم المُوثق أو المشاهد المُوثق بالوصول إلى الموقع الإلكتروني أو البريد الإلكتروني عن بُعد. والهدف من هذا الرمز الضار هو إعادة توجيه طلب المُستخدم إلى عنوان URL ذا مهمة خاصة. في الواقع، يُعد هذا النوع من الهجمات خطرًا جدًا ويصعُب اكتشافه، لأن هذه العملية تتم بالكامل بدون علم المُستخدم.

مثال

تخيل أن المُستخدم يُريد أن يتحدث مع صديقه على شبكته الاجتماعية المُفضلة على الإنترنت مثل (www.socialnet.net) للإسف فإن هذه المواقع تسمح لمُستخدميها بإدخال صورهم على الموقع مثل المنتديات أو الشبكات الاجتماعية مثل الفيس بوك.

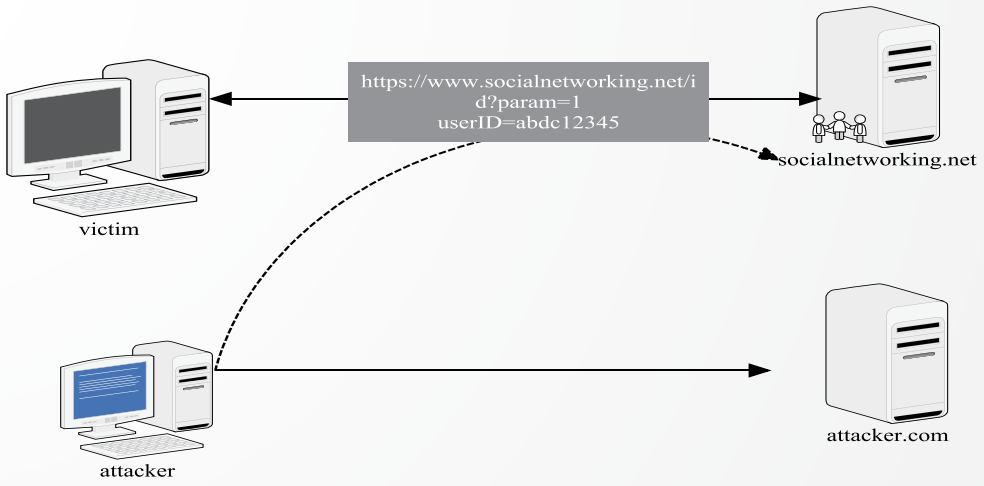


Figure 1: example on how the CERF attack would happen.

الإجراء الطبيعي الذي يُمكن اتخاذه في هذه الحالة: (طريقة المستخدم):

<img src=http://socialnetworking/image.jpg >

الطريقة التي يتبعها المُهاجم:

<"img src=http://socialnetworking/changepassword?newpassword=password12345 >

توضيح : شكل1: مثال يوضح كيفية حدوث هجوم CSRF

هناك العديد من الطرق التي يستخدمها المهاجم لتنفيذ هجمه CSRF واشهرها هو استخدام علامه صورة HTML او صور جافا سكربت. مثل ما اوضحت سابقا فان المهاجم يضع العلامات في ايميل او موقع الكتروني , وبدون معرفه المستخدم , يقوم بتحميل اي صفحه او ايميل يطلبها المهاجم المتصل. بالاسفل نري قائمه بالطرق الشائعه التي يمكن ان يستخدمها المهاجم ليحاول ارسال الطلب.

HTML Methods
IMG SRC
<img src="http://host/?command">
SCRIPT SRC
<scriptsrc="http://ost/?command">
IFRAME SRC
<iframesrc="http://host/?command">

JavaScript Methods

'Image' Object

```
<script>
var foo = new Image();
foo.src = "http://host/?command";
</script>
```

'XMLHTTP' Object (See "Can applications using only POST be vulnerable?" for when this can be used)

IE

```
<script>
var post_data = 'name=value';
var xmlhttp=new ActiveXObject("Microsoft.XMLHTTP");
xmlhttp.open("POST", 'http://url/path/file.ext', true);
xmlhttp.onreadystatechange = function ()
{
if (xmlhttp.readyState == 4)
{
alert(xmlhttp.responseText);
}
};
xmlhttp.send(post_data);
</script>
```

كيف يُمكنك تفادي هذه الهجمات؟

عد توضيحنا لمعنى هجمات CSRF وطرق تفكير المُهاجمين، يجب أن تعرف الآن كيف يُمكنك حماية نفسك منها.

شخصيًا انصحك بمراجعة sheet OWASP CSRF attack prevention cheat ويُمكنك أن تجدها في موقع:

https://www.owasp.org/index.php/CrossSite_Request_Forgery_%28CSRF%29_Pre-[
[vention_Cheat_Sheet

ويُمكنك أن تجد أيضًا في موقع OWASP العديد من الأدوات التي يُمكن أن تُساعدك في اختبار الأكواد ويُمكنك معرفة أكثر عن هجمات أخرى مختلفة بالتفصيل.

في الواقع إذا أردت أن تبحث على الإنترنت عن طرق حماية نفسك من هجمات CSRF ستجد مئات الملايين من المقالات والصفحات الإلكترونية التي ستعطيك العديد من الاقتراحات. لكن إذا بحثت بدقة أكبر ستجد أن هناك الكثير من المفاهيم الخاطئة حتى في أفضل المقالات، وقد قام إيريك شيريدان بمناقشة هذا (وهو أحد أفراد الفريق الذي قام بمراجعة تطورات أعلى 10 نقاط ضعف في تطبيقات الإنترنت برعاية موقع OWASPويُمكنك معرفة المزيد من المعلومات في الموقع [https://www.owasp.org/index.php/Top_10_2010])، وستكون كالآتي:

Figure 2: example on HTTP Referrer [4]

1. اقبل ما نُشر فقط:
- يؤدي ذلك إلى وقف الهجمات البسيطة المُعتمدة على الروابط (IMG, frames.....)
- لكن يُمكن إنشاء خبر (post) مخفي داخل الإطارات والسكربت وغيرهم.

2. مراجعة الإحالات:
- بعض المُستخدمين يحظرون الإحالات لذا لايُمكنك طلب عنوان إحالة.
- التقنيات لخلق طلب HTTPمختار بدون وجود إحالة.

3. النقل يتطلب خطوتين:
- يُمكن لهجوم CSRF أن يضيف خطوة في الطلب.

4. إعادة كتابة URL:
- الكشف عن رقم الاتصال العام في السجلات والذاكرة التخزين المؤقتة وغيرهم.

الاستنتاج:

خطورة هجومCSRF والتي تستهدف بياناتنا المالية والصحية وحواسبنا وتسمح للمُهاجم باستغلال التنقلات الرسمية التي يقوم بها المُستخدم. مثل ما أوضحت سابقًا يُمكنك أن تجد حسابك البنكي ينقل الأموال لحساب آخر بمعرفتك أو كلمتك السرية لأي تطبيق على الإنترنت معروفة ويُمكنك رؤيتها. تكمُن خطورة هذه الهجمات في أن كل التنقلات التي يقوم بها المُهاجم رسمية.

للمعرفة:

ومن هنا أُصرح أن معظم هذا المقال له مراجع من كُتاب آخرين بالإضافة إلي أن الأكواد المذكورة أعلاه مأخوذة من موقع إلكتروني آخر مذكور في قسم المراجع. بالإضافة إلى أنني أحب أن أشكر فريق التحرير بسبب جهوده لإخراج هذا العمل إلى الضوء. إذا كنت تريد إعطاء أي ملاحظات او تعليقات أو أسئلة، أرجو المُراسلة على البريد الإلكتروني: Ahmed.neil@owasp.org

عن الكاتب: أحمد نيل هو قائد قسم OWASP في المنصورة- مصر. وهو باحث في أمن المعلومات في كلية حاسبات ومعلومات جامعة المنصورة في مصر. وقد قام بتنظيم العديد من المناسبات الخاصة بمجال أمن تكنولوجيا المعلومات للتوعية والاهتمام بكل مايخص أمن المعلومات. بالإضافة إلى عضويته في العديد من نوادي أمن المعلومات.

المراجع وإضافة معلومات:

1. [OWASP [https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29
2. [Robert Auger @ [http://www.cgisecurity.com/csrf-faq.html
3. [http://haacked.com/archive/2009/04/02/anatomy-of-csrf-attack.aspx]
4. [#http://knol.google.com/k/preventing-cross-site-request-forgeries-csrf-using-modsecurity]
5. [/http://evilzone.org/tutorials/csrf-tutorial-by-connection]
6. [/http://www.gnucitizen.org/blog/csrf-demystified]
7. Eric Sheridan, Cross-Site Request Forgery: Danger, Detection, and Defenses, can be found on OWASP
8. [http://www.techrepublic.com/blog/networking/csrf-attacks-home-dsl-routers-are-vulnerable/756]
9. Jesse Burns, Cross Site Request Forgery , An introduction to a common web application weakness, can be found in https://www.isecpartners.com
10. Kurt Seifried, Attack of the CSRF, 2008

Ahmed Nile

I am the OWASP Mansoura– Egypt chapter leader. Neil is an Information Security researcher in the Faculty of Computer and Information Sciences at Mansoura University-Egypt.

BLUE KAIZEN
Online Store

If You like our magazine and our activities help us to continue producing it by giving an amount of your liking.

Opening Soon

SecurityKaizen magazine

نقاط الضعف = فرص

تُعد نقاط الضعف فرص لمُتخصصي المعلومات الأمنية سواء كنت إنسان جيد أو سيء.

لو كنت قرصان فهذه هي فرصتك الذهبية لتحقق حلمك وتصل للمجد في القرصنة، أما إذا كنت مسؤول أنظمة أو شبكات فهذه هي الفجوات التي تحتاج لتغطيتها.

تعني نقاط الضعف لمسؤولي الشبكات (على الأقل الجيدين منهم) "أخيرًا بعض العمل الحقيقي" على الأقل أفضل من إعادة ضبط كلمة المرور "أو ما يُعرف بالإدارة العليا" للمُستخدمين الحمقى الذين ينسون مفتاح تثبيت الحروف الكبيرة CAPS Lock يعمل بعد 6 محاولات.

ويبقى السؤال...كيف تجد نقاط الضعف؟
القراصنة المحترفين يتبعون طريقة تُسمى Triage لجمع المعلومات عن هدفهم. تلك المعلومات تُساعدهم لتحديد وإجابة بعض الأسئلة مثل:

- ما هو نظام التشغيل الذي يقومون باستخدامه؟
- ما هو مستوى أنظمة الحماية عند الهدف؟
- ما هي الأنظمة التي يقومون باستخدامها (Cisco أو Linksys أو Microsoft...أو أي أنظمة أخرى)؟
- هل يمتلكون كاميرات مراقبة أمنية مُتصلة بالشبكة قد تتيح لك إلقاء نظرة داخل الشركة؟
- هل لديهم طابعات يُمكن استخدامها عن طريق الإنترنت؟

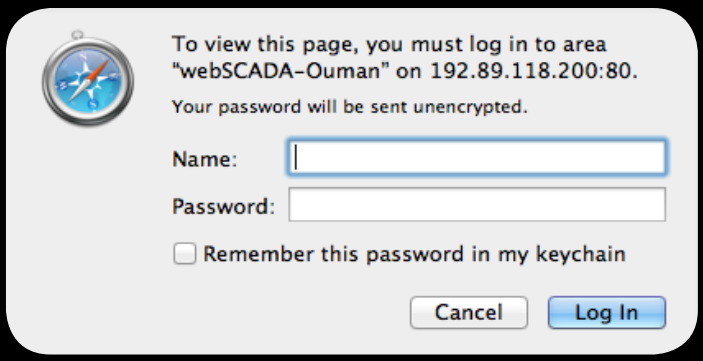
وأخيرًا وبعد أيام من البحث يستطيعون تحديد مدى ضعف الهدف.
بعد ما قلته، لم أتخيل أنه سيأتي اليوم الذي يقوم فيه مُحرك بحث كامل بعمل ذلك لأي قرصان أو حتى لمُتخصص فضولي.
ولكنني قابلت Shodan من سنتين: www.shodanhq.com

ويُعد Shodan مُحرك بحث عن الكمبيوتر على الإنترنت الذي يُمكنك من إيجاد مركز خدمة / أجهزة توجيه (راوتر) / طوابع / كاميرات مراقبة..... وغيرها باستخدام كلمات بحث بسيطة مثل (المنافذ، سيرفر، الشركات، أسماء الشركات... إلخ)

عندما كتبت كلمات بحث مثل: cisco country عاد لي بـ 1409 عنوان IP لأجهزة Cisco التي يُمكن الوصول إليها عن طريق الإنترنت في مصر. لماذا لا تُمضي بعض الوقت لتجربة أسماء وكلمات المرور الافتراضية لترى ماستصل إليه... ستُدهشك النتائج.
عندما كتبت FTP country حصلت على 9373 مركز خدمة FTP في مصر، وتمكنت من الدخول إلى بعضهم فقط عن طريق الدخول كضيف، مما أصابني بالإحباط لأيام.

من 9373 مركز خدمة FTP بعض الشركات تستخدم النسخة الأصلية المُستخدمة في مركز خدمة FTP بدون أي تعديل مما يجعله أسهل للقرصان لإيجاد نقاط الضعف المُتاحة في هذه النسخة بكل بساطة.
في المثال السابق، "مصر للطيران" شركة الطيران المصرية تكشف أن لديهم جهاز CISCO وأن رقم عنوان الـ IP هو: 217.139.100.1 ونوع مركز خدمة FTP ونسخته (1.00) وهي نسخة معروف وجود نقاط الضعف بها. يُعد مركز الخدمة هذا أما أن يكون غير مهم أو ذو قيمة كبيرة.
تملك شركة "إليكو مصر" للتأمين مركز خدمة FTP يُمكن الدخول إليه عبر الإنترنت ولكنه لا يقبل حسابات غير معروفة وهذا شئ جيد على المستوى الأمني.
ويُمكنك أيضًا تجربة استعلام سيوصلك لكل مراكز الخدمة التي مازالت تستخدمIIS 6.0 (مراكز خدمة الويب) في مصر، مثلاً:
عندما تكتب 302- 403- 404- IIS 6.0 والبلد: eg ستجد 2443 مركز خدمة في مصر يستخدم Microsoft IIS 6.0 مع عيوبه ونقاط ضعفه المعروفة منهم على الأقل 8 مواقع حكومية.
هل تسائلت يومًا عن عدد من يزال يستخدم IIS 5.0يُمكنك أن تسأل Shodan.
عندما تكتب 302- 403- 404- IIS 5.0 والبلد: eg ستجد 526 مركز خدمة إنترنت منهم موقع الجامعة الأمريكية في مصر AUC التي ما زالت تستخدم IIS 5.0 الذي صدر مع Windows 2000 منذ حوالي 12 سنة. بالتأكيد تستطيع AUC أن تطور موقعها!
ويوجد مكان آخر يتم استخدام IIS 5.0 فيه ويستحق الملاحظة وهي شركة اوبتيما لتدوال الأوراق المالية (http://41.205.125.68/) وموقعها الإلكتروني ضعيف حيث يحتوي على معلومات مهمة تخص العملاء. إنني أتساءل عن الشخص الذي يقوم بمراقبة نُظم حماية المعلومات الخاصة في مصر؟
ولكن لأكون عادلاً فهذه المشكلة عالمية حتى عند البحث وكتابة SCADA ستجد أن أكثر من 59 مركز خدمة SCADA متاحين على الإنترنت مثل موقع إلكتروني SCADA في فنلدا الذي تملكه شركة صناعية تسألك عن اسم المُستخدم وكلمة المرور

فقط ثم يُمكنك الدخول، ما جدوى هذه الخطوات ضد هجمات القرصنة؟ إن التجربة هي التي ستُظهر لنا.
إذا كنت تريد أن تُفرغ علبة ورق طباعة في أي مكان، فما رأيك بتجربة ذلك في البحث HP print servers with anonymous FTP access والبحث عن 230-Hewl-ett-Packard فستجد أكثر من 350 طابعة متاحة عبر الإنترنت يُمكنك محاولة الوصول إليها.
إذا كنت تريد أن تتسلى، فيُمكنك أن تجرب البحث عن PelcoNet-Web server وهو مركز خدمة التدفيق الافتراضي لـ Pelco surveillance cameras (كاميرات مراقبة Pelco) وهي أفضل شركة لبيع كاميرات المراقبة الأمنية في العالم وسيمكنك مشاهدة ما يراه الحارس الأمني في الشركة على الهواء مباشرة. أعتقد أن هذه المعلومات ستفيدك إذا كنت تخطط لسرقة بنك.. لكن لا تُخبر أحدًا أنك عرفت هذا عن طريقنا!



Omar Sherin
I am a certified CBCP, CRISC And ISO27001 LA and in my spare time an active blogger in CIIP.Wordpress.com

تلميحات أمنية حول موقع facebook®

نحن نعمل جاهدين في موقع Facebook لحماية الأشخاص الذين يقوموا باستخدام موقعنا. فبدايةً من فريق عمليات المستخدم الخاص بنا الذي يعمل على إعادة تأمين الحسابات المُعرضة للخطر إلى الفريق الهندسي الذي يقوم بتصميم خصائص الحماية الجديدة وتنفيذها مثل إشعارات تسجيل الدخول. ويعمل الجميع على ضمان حصول المستخدمين على تجربة آمنة وممتعة. ويقوم موظفينا وعمليات الاستثمار في المعدات وتطوير أدوات الملكية وخصائص الحماية الاختيارية بمساعدتنا في الحفاظ على أمنك. ولكننا نعلم أن هذه المهمة لا تكون مكتملة أبدًا، ولذا فنحن نستمر في الابتكار.

تلميحات حول حماية موقع الفيس بوك "Facebook Security":

- استخدم أدوات الحماية الخاصة بنا – قم بمراجعة إعدادت الحماية الخاصة بك وقم بأخذ الدخول في تمكين إشعارات تسجيل الدخول وموافقات تسجيل الاعتبار. توجد هذه الأدوات في الصندوق المنسدل ضمن "إعدادت الحساب" في أعلى الحافة اليمنى من صفحة فيس بوك الرئيسية.
- لا تنقر فوق الروابط الغريبة: حتى إذا كانت من أصدقائك، وقم بإخطار صديقك إذا رأيت شيئًا مريبًا.
- لا تنقر فوق طلبات الصداقة من مستخدمين مجهولين
- استخدم روابط الإبلاغ الموجودة في الموقع: إذا صادفت عمليات نصب أو إزعاج فانقر فوق روابط الإبلاغ حتى يتمكن موقع الفيس بوك من إيقافها.
- لا تقم بتنزيل أية تطبيقات لا تثق بها.
- قم بزيارة صفحة الحماية الخاصة بموقع فيس بوك: http://www.facebook.com/security، واقرأ عناصر "إتخاذ إجراءات" و"التهديدات."

إن إدارة موقع الفيس بوك Facebook ملتزمة دائمًا بحماية حسابات ومعلومات الأشخاص الذين يقوموا باستخدام الموقع. ويعمل فريق الحماية الخاص بنا المُكون من 300 عضو على مدار الساعة لإعاقة مُرسلي البريد المزعج والحفاظ على أمن موقع الفيس بوك Facebook. نحن نقوم أيضًا بمعالجة كميات ضخمة من المحتويات كل يوم لحماية مُستخدمي الموقع – ونقوم بمراجعة أكثر من 26 بليون قطعة من المحتويات و2 مليار رابط يتم النقر عليهم يوميًا.

يعمل مهندسينا على التأكد من أن استخدام موقع Facebook يُعد تجربة آمنة من خلال استخدام تكنولوجيا مُتقدمة. يوجد لدينا العديد من الأنظمة التي تعمل في الخفاء لاكتشاف التهديدات وتجريدها وتعطيلها. لقد قمنا بإضافة أدوات لمنع أشكال رسائل الإزعاج المختلفة وقد قمنا أيضًا بتطبيق حماية ضد استخراج البيانات (anti-scraping protection) لضمان بقاء بيانات المُستخدمين آمنة. ونقوم أيضًا بالعمل مع قسم تنفيذ القانون وبالتحقق من 300 مليون صورة يتم تحميلها يوميًا في مقابل قاعدة بيانات محظورة من الوكالات الدولية والفيدرالية والحكومية ووكالات تنفيذ القانون المحلية.

ولكن لا تعمل جميع آليات الحماية في الخلفية ونريد أن نترك للجميع المزيد من التحكم في تجربتهم في موقع Facebook. يوجد لدينا العديد من أدوات التحكم الخاصة بالمُستخدم التي من خلالها يتم استخدام قوة الروابط الاجتماعية للحفاظ على أمن الجميع على الموقع. بعض أدوات التحكم هذه تُعد أجزاء أوتماتيكية في الحساب، بينما تتيح لك أدوات التحكم الأخرى اختيار مستوى الحماية الذي يُناسب أسلوب حياتك بأفضل شكل. نحن نقوم بتشجيع مُستخدمي الموقع على القيام بزيارة صفحة الحماية الخاصة بالموقع "Facebook Security" أو "مركز المساعدة" لمعرفة المزيد حول هذه الأدوات.

وأيضًا نقوم بتسليح الأشخاص الذين يقوموا باستخدام موقعنا بالقوة التي تُمكنهم من حماية أنفسهم. يُمكنك تمكين أدوات التحكم التي ستساعدك على البقاء آمنًا ومُحدثًا بسهولة. وعلى مدار العام الماضي، قد قمنا بإطلاق أدوات مثل "الموافقات على تسجيل الدخول" و"إشعارات تسجيل الدخول" و"كلمات مرور المرة الواحدة" و"التصفح الآمن HTTPS" ونقوم باستمرار بالبحث عن طرق لتعليم المُستخدمين وحثهم على استخدام هذه الأدوات.

نحن راضون عن النتائج التي توصلنا لها حتى الآن للحفاظ على موقع الفيس بوك آمنًا والعمل بجد كل يوم لتحسين الأنظمة والأدوات الخاصة بالموقع. ويتعرض أقل من 0.5٪ من المُستخدمين للرسائل المَزعجة في أي يوم محدد، ويتم تصنيف أقل من 0.1٪ من تسجيلات الدخول كتسجيلات دخول مشبوهة. ومع ذلك، لا نرضى بشكل كامل عن النتائج التي نتوصل إليها ولذا فنحن نكافح دومًا لبناء أدوات وأنظمة إبداعية للتأقلم مع التهديدات الجديدة والرد عليها. نحن نتعامل مع أمن مُستخدمينا وحماية بيانتهم بجدية ونكافح لضمان حصولهم على تجربة آمنة عند استخدام موقع الفيس بوك.

Joe Sullivan
I am the chief security officer of faceebook.com, i manage a few of the teams at facebook focused on making sure that people who use facebook have a safe and positive experience

أحداث مؤتمر القاهرة الأمني 2011

للذين لايعرفون مؤتمر أمن المعلومات (CSCAMP) الذي تم إقامته بالقاهرة فهو مؤتمر سنوي لمُتخصصي أمن المعلومات حيث يجتمع كل الخبراء وغير الخبراء في مكانٍ واحد لمدة يومين لمناقشة ومشاركة المعرفة الأمنية والتكنولوجيا. مؤتمر أمن المعلومات بالقاهرة بدأ عام 2010 بجمع صغير من 80 شخص في جامعة النيل في القرية الذكية. وقد عُقِد المؤتمر في عام 2011 في الجامعة الأمريكية بالقاهرة وبلغ الحضور أكثر من 300 شخص من المتخصصين الأمنين من القاهرة والشرق الأوسط. وللحصول على معلومات أكثر عن مؤتمر أمن المعلومات بالقاهرة يُرجى زيارة موقعنا (www.bluekaizen.org).

ويُعد المؤتمر هذا العام تجربة فريدة وجديدة لكل شخص مُهتم بأمن المعلومات في مصر والشرق الأوسط. فقد استطاع جميع الحضور الانخراط بحرية في المجتمع العبقري ومقابلة أشخاص جُدد ومعرفة معلومات جديدة والاستمتاع في الوقت ذاته. هذا بالطبع بدون ذكر مشاهدة مسابقة التقاط العلم المعروفة عالميًا بـ "Capture the Flag" لأول مرة في مصر والتي تقيس مهارات المُتميزين في مجال أمن المعلومات في تقييم واختراق دفاعات ظظام معلومات المسابقة والحصول على ملف خاص يُثبت نجاح هذا الاختراق والراعي الرسمي لهذه المسابقة syn-apsLabs.

بدأ اليوم الأول من المؤتمر بالتسجيل وتكوين فِرق المتنافسين في مسابقة "التقاط العلم" (CTF) مُصاحبةً مع التسجيل لحضور المؤتمر وتوزيع العدد الأخير من مجلة سيكيورتي كايزن.

وقد بدأ معتز صلاح مؤسس مؤتمر أمن المعلومات بالقاهرة بعد صلاة الجمعة بإلقاء كلمة عن المؤتمر وقد عبر عن مشاعره تجاه المؤتمر كإبن ثانٍ له ويجب على الجميع الاهتمام به ودعمه والتغاضي عن أخطاءه مثلما يُعامل الأب صغيره حتى يقف على قدميه ويستطيع الركض كبطل رياضي.

وبعد ذلك، بدأ كريس بروان الكلمة الافتتاحية في اليوم الأول، مدير عمليات EMEA Operations NetWitness

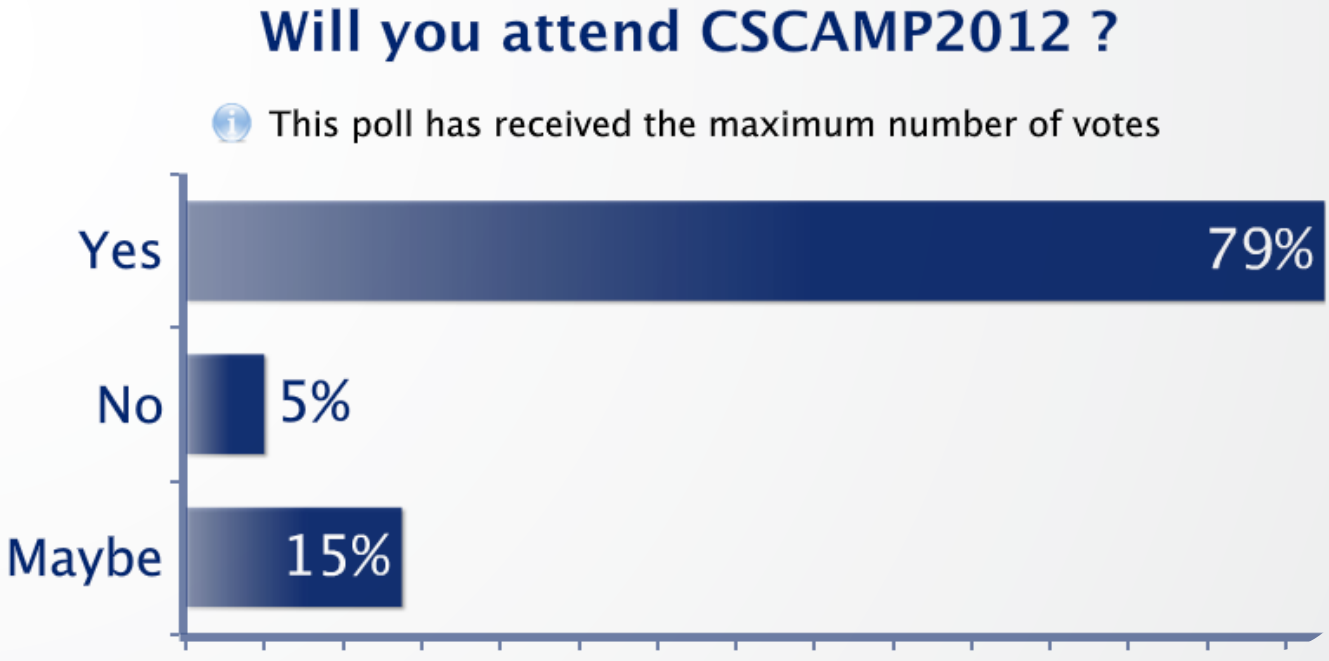
بشركة RSAوكانت كلمته عن سبب اختفاء الحلول الذهبية لمكافحة الفيروسات. وبعده تحدث أ\ سامر عُمير المدير العام بشركة Qualys وتحدث عن تأمين الحوسبة السحابية وتحدث بعده باقي المُتحدثين.

وقد بدأ اليوم الثاني بالكلمة الافتتاحية للدكتور شريف هاشم مستشار وزير الاتصالات وتكنولوجيا المعلومات للأمن الإلكتروني ونائب المدير التنفيذي بهيئة تنمية صناعة تكنولوجيا المعلومات المصرية ITIDA وتلت محاضرته باقي المحاضرات.

وأحد أكثر المحاضرات التي جذبت انتباه الحضور هي محاضرة عمر شيرين. عمر شيرين هو مدير حماية معلومات البنية التحتية الهامة في QCert وكان عنوان محاضرته أمن SCADA والأخطار الناشئة. وقد حصلت المحاضرة على المركز الأول في التقييم للمؤتمر وقد حصل على أعلى النقاط في كل شئ مثل: تعريف المُتحدث ومهارات التقديم والموضوع وشرائح العرض. وقد ذكر أيضًا التهديدات الرئيسية لأنظمة SCADA في مصر. وننصح بمشاهدة الفيديو للمُهتمين على موقعنا www.bluekaizen.org. ومن المُحاضرات المُتميزة أيضًا الكلمة الختامية التي قدمها أسامة حجي وأحمد العزبي بعنوان "أمن المعلومات ومستقبل مصر" وتحدثوا فيها عن مستقبل أمن المعلومات في مصر بعد 25 يناير وكيف يُمكننا اتخاذ خطوات سريعة في عملية إصلاح مشاكلنا في أمن المعلومات. وقد قام أسامة وأحمد بالتركيز على قانون حرية الاتصالات وحق كل شخص في أن يتم السماح له بالاتصالات وتجنب ماحدث أثناء الثورة من قطع الإنترنت وشبكات المحمول. وقد كان اختيار المواضيع والمناقشات موفقًا كختام لمؤتمر أمن المعلومات بالقاهرة CSCAMP2011.

وفي نهاية المؤتمر، تم توزيع هدايا بشكل عشوائي على الحاضرين بما في ذلك 5 اشتراكات مجانية لمجلة الاختراق المشهورة و3 دورات تعليمية في CEH v7 من المجلس الدولي لاستشارات التجارة الإلكترونية وغيرهم. ووزعت هدايا قيمة للفائزين بمسابقة CTF مثل دورات مجانية وقسائم امتحان مجانية من أكاديمية راية وغيرها.

وقبل المغادرة، اهتم معتز صلاح بالحصول على التقييمات من الحاضرين ولذلك قام بإجراء استقصاء للمُستخدمين عن نيتهم لحضور مؤتمر CSCAMP2012 أم لا. يُمكنك رؤية شكل1 للنتائج.
وقد كان ٪79 من حوالي 80 مُستخدم أجاب عن الاستقصاء يريدون حضور المؤتمر في عام 2012 بينما أجاب ٪5 أنهم لا يريدون الحضور و٪15 أنهم ربما يحضرون



وختامًا، على الرغم من أن مؤتمر القاهرة لأمن المعلومات CSCAMP2011 هو مجرد محاولة صغيرة للوقوف والتحرك لكننا تلقينا العديد من التقييمات الإيجابية والتعليقات الداعمة للمؤتمر على تويتر باسم #CSCAMP2011 وأيضًا على صفحتنا على الفيس بوك والتي جعلتنا واثقين أن هذا المؤتمر وُلد ليعيش ويبقى أحد أهم المؤتمرات لأمن المعلومات في الشرق الأوسط. يجب عليك ألا تُفوته.

CSCAMP 2012

WWW.BLUEKAIZEN.ORG

Securitykaizen

التعليقات:

أدهم (أحد الفائزين في مسابقة CTF) قال:

"لقد قضيت وقتًا طويلاً في البحث عن مسابقة أو تحدي في مجال أمن المعلومات كي أتمكن من تقييم خبراتي وأقابل أشخاص مُهتمين بأمن المعلومات مثلي. وقد أنهيت هذا البحث عندما عرفت بمؤتمر القاهرة لأمن المعلومات [CSCAMP2011]. وأحد أهم الأشياء التي جعلتني أنضم للمؤتمر هو وجود تحدي CTF متعدد المراحل والمتطلبات الأساسية للمرحلة من مستويين من JavaScript التي تقيس طريقة تفكيرك وقدرتك على إيجاد حلول للمواقف. لقد كان هذا ممتعًا جدًا. وبالطبع كنت قلقًا إلى حدٍ ما في البداية لإنها أول مرة اشترك في مسابقة CTF حقيقية لكن المُنظمين كانوا ودودين ومتعاونين ويتحدثون معنا دائمًا. لا أستطيع وصف السعادة والمتعة التي شعرت بها خلال اليومين في كلمات. وقد حصلت الفرق الفائزة على جوائز تراوحت مابين خصومات كبيرة لدورات أمن المعلومات أو دورات مجانية وأيضًا الفرصة للسفر للمرحلة الثانية من المسابقة في دبي. لم يخرج أحد من المسابقة خاسرًا، فمعرفة الزملاء الرائعين في المجال ومقابلة الأشخاص الجُدد هي الهدية الحقيقية."


改善
BLUE KAIZEN
Connecting Minds Improving Lives
Are you interested to know about hacking incidents
New Events | New Technologies
Online
News
2day adv.
An up to date link with the security community bk news is your way
www.bluekaizen.org/bknews.php

Abu Dhabi
CYBER DEFENCE
SUMMIT مؤتمر الأمن السيبراني

تم استضافة مؤتمر "قمة الدفاع الإلكتروني" هذا العام في أبو ظبي، عاصمة دولة الإمارات العربية المتحدة في فندق راديسون بلو في جزيرة ياس. يدور محور هذه القمة حول موضوع "حماية الممتلكات الهامة من التهديدات الإلكترونية." وقد تميزت هذه القمة بخطابات رئيسية ومداولات ومناقشات جماعية واجتماعات فردية ذات مستوى رفيع. وقد أستقبل الاجتماع بشكل جيد بواسطة كافة المديرين التنفيذين في دولة الإمارات العربية المتحدة والشرق الأوسط. وكان غالبية الحاضرين من العاملين بالوزارات مما يدل على التزام قيادة الدولة تجاه حماية الفضاء الإلكتروني وحماية الممتلكات القومية الهامة.

وقد تضمن اليوم الأول: العناوين الرئيسية
* قام فيليب فيكتور مدير السياسات والتعاون الدولي في الشراكة الدولية متعددة الأطراف ضد التهديدات الإلكترونية (IMPACT) بتقديم الخطاب الافتتاحي.

* مداولة حول دور مركز الاستجابة لطوارئ الحاسب الآلي (سيرت CERT) وأهميته وقد شارك فيها (مركز الاستجابة لطوارئ الحاسب الآلي AE Cert بدولة الإمارات ومركز الاستجابة لطوارئ الحاسب الآلي Oman CERT بدولة عُمان)

* قام ماركو دونفرانشسكو – رئيس استراتيجية المنتجات الخاصة وسيليكس للأنظمة المتكاملة- بتقديم خطاب رئيسي حول الدرع الإلكتروني المتكامل.

تميز اليوم الثاني بـ: المحاضرات والعروض التقديمية

* قام كارل وليامسون – المدير التنفيذي لـ Cyber Strategy Defense Enterprise Solutions، شركة وورثروب جرومان (Northrop Grumman Corpo-ration) – بتقديم خطاب رئيسي حول التخطيط المُستقبلي لضمان مؤسسة محمية إلكترونيًا.

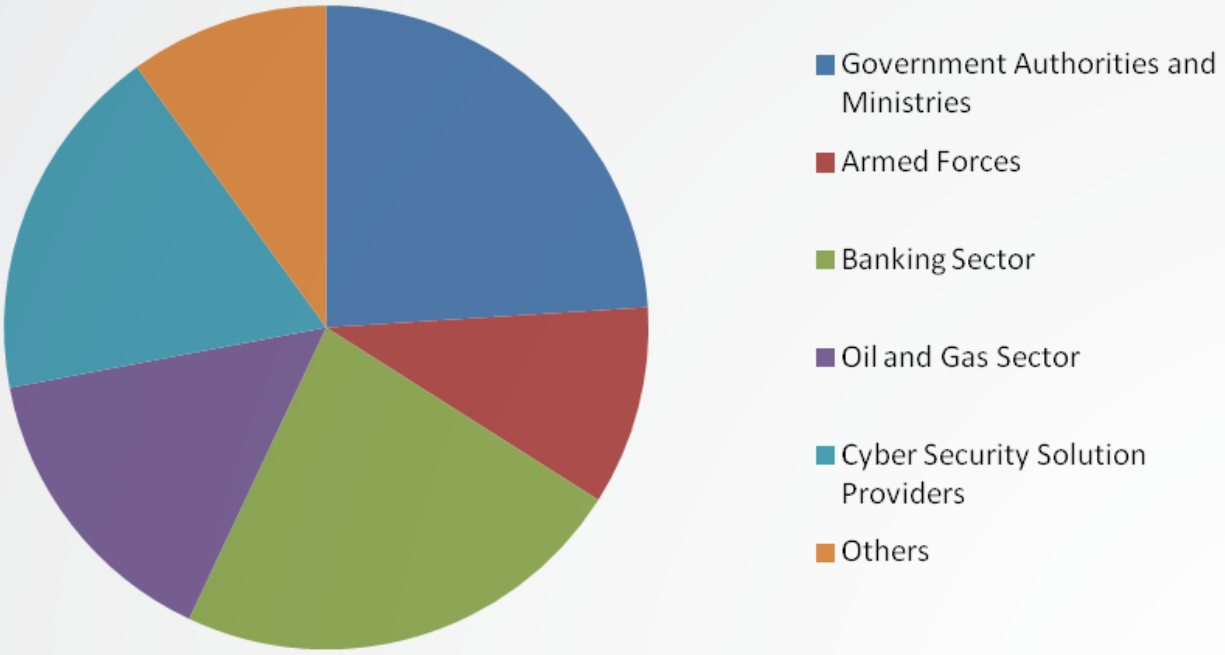
* مداولة حول التهديدات والتحديات الخاصة بتكامل الحوسبة السحابية للقطاع العام.

* وقد دارت مناقشات جماعية حول مستقبل الحماية الإلكترونية في GCC، وجدوى التعاون والمشاركة في المعلومات القومية والدولية.

لقد حضر هذا الحدث العديد من الموفدين من قِبل القوات المسلحة وصانعي القرار الحكوميين والعاملين والمديرين التنفيذيين من مؤسسات مختلفة.

يتمثل قطاع مستعرض من الجمهور في الشكل الموضح أدناه.

Sector Wise Audience Split Up



A cross section of the audience is represented below.

ملخص النتائج التنفيذية:

لقد كانت نتائج الحدث واضحة جدًا ويُمكن تلخيصها كما يلي أدناه.

1. آليات تبادل المعلومات الاستخبارية أكبر على المستويات الوطنية والدولية.
2. الحاجة إلى منتدى مركزي للبحث في التهديدات الأمنية للإنترنت.
3. الإنسان هو الحلقة الضعفية في سلسلة الأمان ويحتاج إلى تقويته عن طريق التدريب وبرامج الوعي المستمرة.
4. الحاجة إلى برامج للوعي بالأمن الإلكتروني الوطنية عن طريق الفرق المُتخصصة.
5. الحاجة إلى إنشاء نقاط اتصال مركزية على مستوى الشركات لمشاركة وتقليل أخطار الأمن الإلكتروني.
6. الحاجة إلى بناء استخبارات لمراقبة البيانات التي يتم تداولها على الشبكات.
7. الحاجة إلى اتباع نهج استباق للهجوم بدلاً من نهج رد الفعل الدفاعي.
8. الحاجة الكبيرة إلى زيادة الأمن في سلاسل الإمدادات.

الاستنتاج

أخيرًا وليس آخرًا ومع زيادة مخاطر الأمن الإلكتروني بمعدل خطير والخسائر التي تحدث في الشرق الأوسط وحده التي تبلغ حوالي 1.44 بليون درهم للتعامل مع حوادث الأمن الإلكتروني. فإن مواجهة التهديدات الأمنية الإلكترونية تحتاج إلى نهج متكامل يضم الناس والعمليات والتكنولوجيا والتعاون الدولي. وقد تم تأييد هذا من قِبل كل فرد حضر المؤتمر.

حوادث الاختراق في مصر والشرق الأوسط

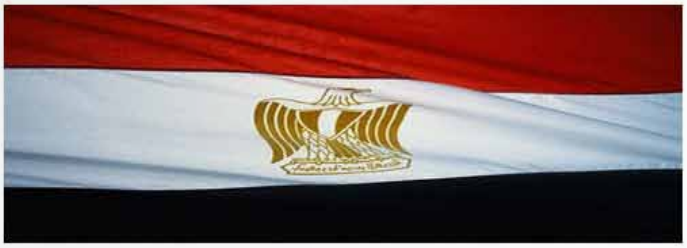
اختراق راديو إسرائيل

تخريب موقع رئيس الوزراء الإسرائيلي نتينياهو بواسطة مُخترق مصري

في العشرين من أغسطس 2011، قام أحد المُخترقين المصريين يوم الأحد باختراق الموقع الإلكتروني الخاص برئيس الوزراء الإسرائيلي، بنيامين نتينياهو، وقام بوضع صورة للجنود مصريون يرفعون علم مصر فوق أرض سيناء أثناء حرب السادس من أكتوبر 1973 على الصفحة الرئيسية الخاصة بالموقع. وقد كتب المُخترق الذي نجح باختراق الموقع على الصفحة الرئيسية "ضد الصهيونية،" ثم بعد ذلك تم إغلاق الموقع بالتدريج.

www.radiolink.co.il

-: Message By Egytian H4x0rZ :-



```
Hi to greatest son of the bitches of the world ...
This Msg From Egypt " Mother Of The World "We Never Forgot And Never
Forgive Any Isrealian Bitch3Z you Started The War Attack Us On The
borders of Egypt For Nothing Reason .. So You Have Bear Our Attacks
Fuck To All Isreal ./3x!t
.....
```

Mego : EG5-@hotmail.com

Soly : i-7@hotmail.fr

Elga7ed : F7Y@live.com

قام المُخترق المصري بتخريب الموقع الإلكتروني الخاص بالراديو الإسرائيلي وقام بكتابة رسالة على الصفحة الرئيسية، كما هو موضح أدناه:

أهلاً بأكثر البشر نذالة في العالم أجمع... أقوم بإرسال هذه الرسالة إليكم من مصر "أم الدنيا" فنحن لا ننسى ولا نُسامح أبدًا أي وغد إسرائيلي فأنتم من بدأ بالحرب وبمُهاجمتنا على الحدود المصرية بلا أي سبب.. ولذا يجب عليكم أن تتحملوا هجماتنا أيضًا

تبًا لجميع الإسرائيليون

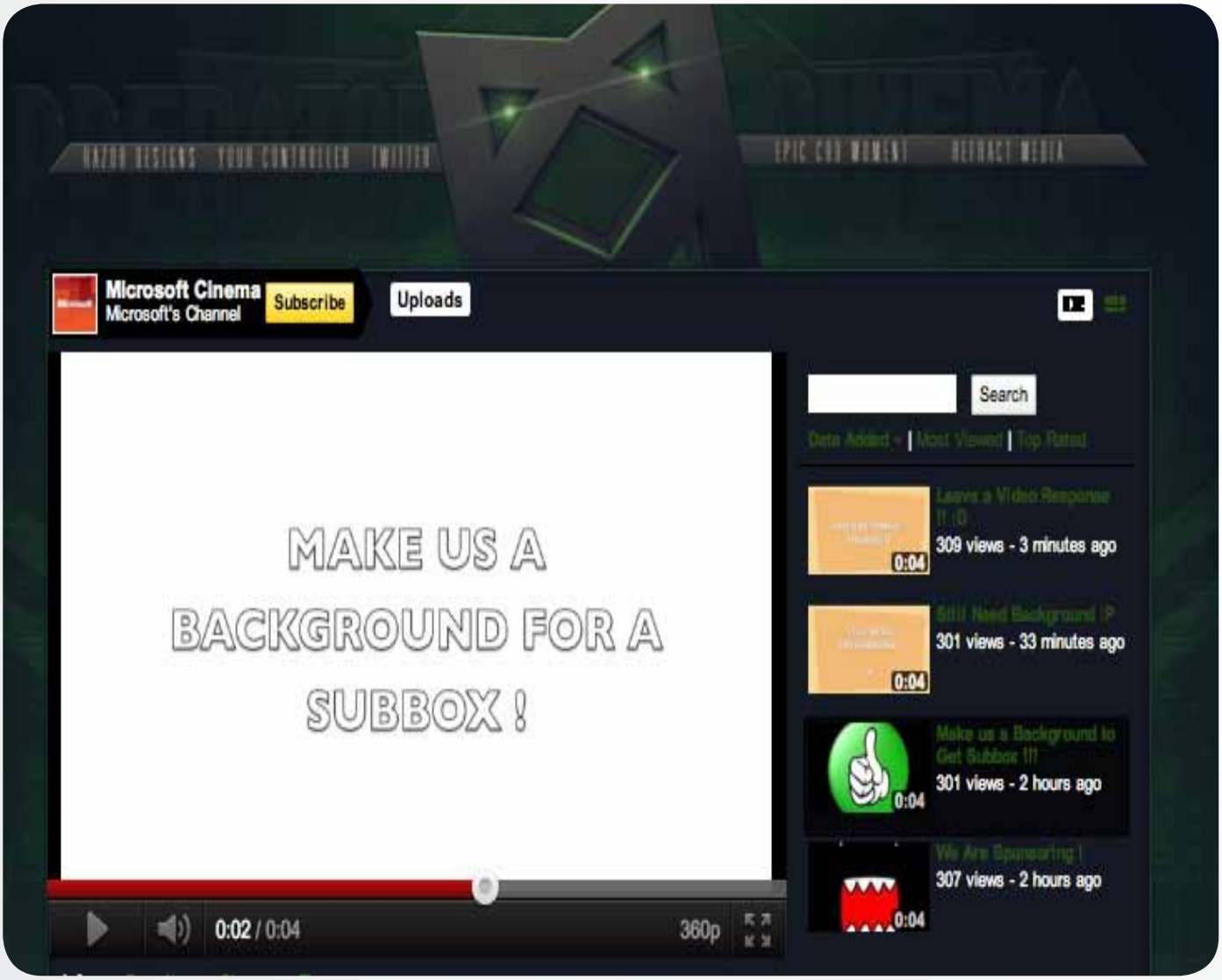
اختراق صفحة فودافون مصر على موقع الفيس بوك ثم اختفائها

قامت مجموعة من المُخترقين المصريين – تُسمى "توراندو المُدمر" (Destructive Tornado) - باختراق صفحة فودافون مصر على موقع الفيس بوك وقد قامت بتغيير صورة العرض الخاصة بالصفحة ونشر تعليقات تُعلن تحكمهم في لوحة التحكم الخاصة بالصفحة. وقد جاء هذا الفعل كتعبير عن الغضب المصري لعمبية قطع الاتصالات التي تمت في الخامس والعشرون من يناير الماضي. وقد حظت الصفحة بالمزيد من الشهرة بشكل سريع بالعديد من التعليقات لصالح المُخترق و"شُكره" كنوع من السخرية لحملة "شكرًا" من شركة فودافون. ومع ذلك، ولبعض الأسباب فقد قرر المُخترق القيا بحذف الصفحة التي تحتوي على 800.00 مُعجب. ولكن لم يأخذ الموقف الكثير من الوقت حتى قام فريق التواصل الاجتماعي من فودافون بالقيام بإلقاء بيان وإعادة إنشاء صفحة الفيس بوك الخاصة بالشركة مرةً أخرى لكَسب 1155 مُعجب.

ووفقًا لفودافون مصر فإن المُخترق قام بالتحكم بالصفحة لمدة 45 دقيقة والتي أيضًا تمكن من الوصول إلى "الرسائل" الخاصة بها والتي تحتوي أرقام هواتف العملاء الذين يقومون باستخدام موقع الفيس بوك لإرسال الشكاوي وأرقام الهواتف.

اختراق قناة مايكروسوفت على موقع YouTube

يبدو أنه قد تم اختراق القناة الرسمية لشركة مايكروسوفت على موقع Youtube صباح يوم الأحد. وقد تم حذف جميع مقاطع الفيديو الرسمية بما في ذلك إعلانات الحملات الأخيرة من الحساب. وعلى نحو لا يدعو إلى الاندهاش، تم استبدالهم بمقاطع فيديو صغيرة لاجتذاب المُعلنين حيث يوجد 24.000 مُشترك في القناة. وقد تم رفع 4 مقاطع فيديو على الحساب بدءًا من الساعة 1:30 ظُهرًا بالتوقيت الشرقي وقد تم وضع علامات زمنية عليها خلال الساعتين الماضيتين. ويبدو أنه قد تم حذف مقطع الفيديو الخامس الذي تم رفعه مؤخرًا. وقد أظهر مقطع الفيديو - "Garry's Mod – Escape the Box" – ما يبدو أن يكون قاتل مُسلح متحرك يقوم بالتصويب داخل أحد صناديق البناء.



حـــوار مـع د/ شريف هاشم

كبير مُستشاري وزير الاتصالات وتكنولوجيا المعلومات للأمن الإلكتروني، ونائب الرئيس التنفيذي لهيئة تطوير صناعة تكنولوجيا المعلومات (ITIDA)، بمصر.

معتز: هل يُمكنك تقديم نفسك إلى قُراء مجلة سيكيورتي كايزن؟

د/ شريف: أنا كبير مُستشاري وزير الاتصالات وتكنولوجيا المعلومات للأمن الإلكتروني ونائي الرئيس التنفيذي لهيئة تطوير صناعة تكنولوجيا المعلومات (ITIDA)، بمصر. وأقوم أيضًا بالتدريس في كلية الهندسة بجامعة القاهرة (في إجازة). وقد حصلت على بكالوريوس في مجال الاتصالات والهندسة الإلكترونية (بدرجة امتياز مع مرتبة الشرف) وماجستير في الريلضيات الهندسية من جامعة القاهرة (مصر – 1985 و1988)، ودكتوراة في الهندسة الصناعية من جامعة بوردو (الولايات المتحدة الأمريكية – 1993). وقد أكملت أيضًا برنامج كبار المديرين التنفيذيين في كلية إدارة الأعمال من جامعة هارفارد (الولايات المتحدة الأمريكية – 2001). وحاليًا أنا مسؤول عن التوقيع الإلكتروني والأمن الإلكتروني وحماية حقوق الملكية الفكرية (IPR) الخاصة بالبرامج وقواعد البيانات. وتشتمل مسئوليتي على إعداد إطار العمل لتأسيس وتشغيل فريق استجابة طوارئ الحاسب الآلي المصري (EGCERT) في الهيئة الوطنية للاتصالات التنظيمية وسُلطة مصدر الشهادة الرقمية المصرية (Root-CA) ومكتب حقوق الملكية الفكرية (IPR) الخاصة بالبرامج في هيئة ITIDA.

By Mostafa Salah

معتز: ما هي الفوائد التي تُقدمها هيئة ITIDA لمجتمع أمن المعلومات على وجه الخصوص، ولمجال تكنولوجيا المعلومات بشكل عام؟

د\ شريف: إن هيئة ITIDA هي المسؤول الأساسي عن التوقيع الإلكتروني في مصر، وحاصلة أيضًا على على شهادة المفتاح العام (Root PKI Certificate Authority - Root CA) للدولة. وترتبط شهادة Root CA ثلاث مُشغلين خدمة شهادة التوقيع الإلكتروني خاصة (CSPs) بالإضافة إلى الشهادة الحكومية CA التي يتم تشغيلها بواسطة وزارة المالية، ولذا يتم توفير بنية تحتية مُتكاملة لخدمات المفتاح العام PKI وتطبيقات التوقيع الإلكتروني في مصر. وتُعد هذه البنية التحتية ضرورية وأساسية لتأسيس الهويات الرقمية الخاصة بالأفراد وحمايتها بالإضافة إلى المنظمات، والتي تُمهد الطريق إلى مجتمع معلومات مصري أكثر تفاعلاً بمزيد من جودة الحياة المُحسنة. وتُعد البنية التحتية للمفتاح العام (PKI) ضرورية ومُهمة للحصول على تطبيقات توقيع إلكتروني وأعمال إلكترونية متطورة ومؤمَّنة. وتُقدِم شهادة Root CA أيضًا مدخلاً للتعرف على شهادات PKI الرقمية مع البلدان الأخرى، مما يؤدي إلى مما يُسهّل تطبيقات الأعمال الإلكترونية ويُمكِّنها مع المجتمع الدولي. لقد تضمن تأسيس البنية التحتية للمفتاح العام PKI على برامج تدريب وتطوير مهارات شاملة للمُتخصصين العاملين في هيئة ITIDA ومع الحاصلين على شهادة السلامة المهنية (CPS)، والتي لا تقوم فقط بتحسين حماية تشغيل البنية التحتية الوطنية ولكن أيضًا توفر فرصًا لتصدير خدمات المفتاح العام (PKI) المتطورة للمناطق العربية والأفريقية. وقد قامت هيئة ITIDA منذ إنشاءها في عام 2005 بتنظيم ودعم واستضافة العديد من الأحداث وورش العمل مثل ندوة اتحاد الاتصالات الدولية للحماية العربية الإقليمية الإلكترونية والهوية الإلكترونية التي تم إقامتها في القرية الذكية من يوم 18 إلى 20 ديسمبر 2011.

معتز: هل من الممكن أن تقوم بإعطائنا لمحة عامة على حالة وتقدُم مشاريع التوقيع الإلكتروني وشهادة Root CA؟

د\ شريف: لقد تم إطلاق شهادة Root CA في الثامن والعشرون من سبتمبر 2009 وقد ربط ثلاث شهادات السلامة المهنية (CPS) الخاصة بشهادة Root CA بعد ذلك بوقتٍ قصير. وقد قامت هيئة ITIDA أيضًا بتوفير العديد لتطوير رمز سري للمفتاح العام (PKI) الذكي المصري. والشركة التي فازت بالمكافأة المالية قامت بتطوير رمزين سريين للمفتاح العام (PKI): باستخدام وبدون استخدام الإحصاءات الحيوية (بصمة الأصبع)، والتي تم إتاحتها حاليًا في السوق المصري، ويتم أيضًا التسويق لها في الخارج. وقد كانت هيئة ITIDA تحاول إقناع الحكومة لتطوير تطبيقات التوقيع الإلكتروني والمفتاح العام (PKI) مع برنامج الحكومة الإلكترونية، ومع مُساهمي المفتاح في العديد من القطاعات بما في ذلك بالطبع قطاع تكنولوجيا الاتصالات والمعلومات (ICT) والقطاع المصرفي والبورصة.

معتز: لقد كنت رائدًا في تأسيس CERT في مصر، رجاءًا، هل يُمكنك إعطائنا لمحة عامة حول CERT وعن دور EGCERT في الحياة الأمنية المصرية؟

د\ شريف: لقد تم تأسيس CERT المصرية في الجهاز القومي لتنظيم الاتصالات المصرية (NTRA) وقد تشغيلها في أبريل 2009. وهي تعمل لمدة 24 ساعة في 7 أيام من الأسبوع، ويوجد بها 16 مُتخصص يقومون بتوفير مستوى عالي من المراقبة ومع حوادث الأمن لمعالجة الدعم مفتاح

المُساهمين المسؤول عن البنية التحتية لتكنولوجيا الاتصالات والمعلومات (ICT) في مصر. ولقد ساهمت EG-CERT في توفير خبراء ومتخصصين يقومون بالإبلاغ وتقديم التقارير إلى المحاكم في قضايا الأمن الإلكتروني الكبرى مثل: قضية Phish Phry التي تم الكشف عنها في أكتوبر 2009. وقد قامت EG-CERT أيضًا بدعم العديد من المُساهمين داخل الحكومة وقطاعات كل من تكنولوجيا الاتصالات والمعلومات والقطاعات المالية في التعامل مع حوادث أمنية متنوعة، بما فِي ذلك هجمات DDOS وعمليات الاختراق وتخريب المواقع الإلكترونية. ومن الجدير بالملاحظة أن الجهاز القومي لتنظيم الاتصالات المصرية (NTRA) قد قام في العامين 2009 و2010 بإطلاق برنامج تدريب حماية إلكترونية مُتكامل والذي تم توفيره من خلال معهد SANS المشهور، وقد نتج عن ذلك حصول 179 مُتخصص في تكنولوجيا الاتصالات والمعلومات (ICT) في الحصول على شهادات في 38 كيان في القطاع الحكومي وشركات تكنولوجيا الاتصالات والمعلومات (ICT) وشركات CSP والقطاعات المالية والمصرفية والمعاهد الأكاديمية. وبالطبع جميع العاملين في EG-CERT من خريجي هذا البرنامج وقد حصل بعضهم على شهادات متعددة من معهد SANS بتقديرات ودرجات عالية.

معتز: يتعجب العديد من مُتخصصي الأمن لماذا لا يوجد موقع إلكتروني حتى الآن لـ EGCERT أو أي رقم هاتف مُعلن للاتصال بهم في حالة وجود حادثة إلكترونية أو استفسار آمني؟
د/ شريف: ستقوم EG-CERT بإطلاق الموقع الإلكتروني قريبًا ولكن في الوقت الحالي يُمكن الوصول إليهم من خلال الجهاز القومي لتنظيم الاتصالات المصرية (NTRA).

معتز: لماذا تقوم CERT باتباع الجهاز القومي لتنظيم الاتصالات المصرية (NTRA)؟ هل هم مهتمون فقط بمجال الاتصالات؟ ماذا عن المجالات الأخرى مثل مجالات البنوك والغاز والنفط؟
د\ شريف: إن EG-CERT هي حجر الأساس الأول في الاتجاه إلى نهج شامل لاستراتيجية البنية التحتية للمعلومات المهمة \ الأمن الإلكتروني. وستقوم مثل هذه الاستراجيات بتغطية وحماية جميع القطاعات المهمة، بما في ذلك القطاعات التي قمت بذكرها أعلاه.

معتز: هل يوجد لدى EGCERT أو أية كيان حكومي آخر برنامج التوعية الآمنية واضح يستهدف عامة المستخدمين مثل طلاب الجامعات وموظفين الحكومة المختلفين والآخرين؟
د\ شريف: وكما هوموضح أعلاه، قد يكون ذلك في حاجة إلى استراتيجية وطنية شاملة.

معتز: في رأيك، لماذا تم اختراق المواقع الإلكترونية الخاصة بالحكومة أثناء ثورة الخامس والعشرون من يناير وهل يوجد لدينا أي نوع من التدقيق على المواقع الإلكترونية الحكومية؟
د\ شريف: يتم استضافة المواقع الإلكترونية الحكومية بواسطة مزودين متنوعين (في المنزل، مزودين خدمة الإنترنت، إلخ)، وفي بعض الحالات لا يلتفت المُزودين و\أو المُطورين إلى الاهتمامات الأمنية، والتي تجعل بعض المواقع الإلكترونية عُرضة للهجمات ال'لكترونية. وكما ذكرت أعلاه، فنحن في حاجة إلى وجود استراتيجية حماية إلكترونية وطنية شاملة. وعلاوةً على ذلك، نحن أيضًا في حاجة تحسين\تعديل الإطار التنظيمي المُتعلق بالاحتيجات التشغيلية لأنظمة المعلومات الحكومية والعامة.

معتز: لقد تلقيت العديد من التعليقات من المجتمع الآمني المصري بأنهم لا يشعرون بأي تقدُم

في مجال أمن المعلومات في مصر. في رأيك، هل السبب هو قلة مطبوعات حول إنجازات وزارة الاتصالات وتكنولوجيا المعلومات (MCIT) في هذا المجال أم بسبب قلة الإنجازات ذاتها؟

د\ شريف: كما ذكرت أعلاه، فقد قامت وزارة الاتصالات وتكنولوجيا المعلومات (MCIT) بإطلاق CERT (في الجهاز القومي لتنظيم الاتصالات المصرية [NTRA]) وشهادة المفتاح العام PKI ROOT CA (في هيئة ITIDA)، وقد قامت بدعم برنامج تدريب شامل على الحماية الإلكترونية الوطنية لـ 220 مُتخصص في 38 هيئة في الحكومة وشركات تكنولوجيا الاتصالات والمعلومات (ICT) وفي القطاعات المالية. وقد قامت وزارة الاتصالات وتكنولوجيا المعلومات (MCIT) والشركات التابعة لها أيضًا (ITIDA وNTRA وNTI وITI) بدعم العديد من الأحداث وتدريبات ورش العمل وتنظيمها، مثل: مؤتمر Hacker Halted (بواسطة مجلس الاتحاد الأوروبي) والعديد من المُتخصصين الرائدين في مجال الحماية الإلكترونية. نحن نُدرك أن تهديدات الحماية الإلكترونية في ازدياد وتنمو أيضًا توقعاتنا تجاه مجتمع الحماية الإلكترونية. وحتى المُتخصصين في مجال الحماية، سواءًا كانوا في القطاع الحكومي أو القطاع الخاص أو المجال الأكاديمي، فنحن في حاجة إلى زيادة مجهوداتنا المتناسقة لتعزيز جدول الحماية الإلكترونية الوطنية، ولتمديد تواصلنا مع المجتمع، ومحاولة التأثير على صانعي القرارات في جميع القطاعات.

معتز: في الشهور القليلة الماضية، لق كان يوجد العديد من المُناقشات حول التصويت الإلكتروني وعن مدى أمنه، فما هو رأيك في هذا الشأن وهل يُمكن تنفيذه في مصر أم لا؟

د\ شريف: إن استخدام وشركات تكنولوجيا الاتصالات والمعلومات (ICT) في عملية التصويت سوف يقوم بتحسين تجربة المواطن بالتأكيد وتسهيل الاشتراك في التحول الديمقراطي في مصر. وفي هذا الصدد، فقد قامت هيئة ITIDA باستضافة مجموعة مُكونة من 100 مُتخصص من شركات تكنولوجيا الاتصالات والمعلومات (ICT) لتحليل أفضل الممارسات على مستوى العالم وتقديم النُصح للحكومة في نهج شامل للحصول تصويت مُحسن لـ ICT.

وقد تم إجراء العديد من الاجتماعات في شهر مارس إلى شهر أبريل 2011، باستخدام أكثر من 40 وثيقة تم تبادلها وتحليلها. وقد تم تقديم التوصيات النهائية إلى مجلس الوزراء، وقد تم وضع بعض التوصيات في الحسبان. ومع ذلك، فلا يزال يوجد أمامنا طريق طويل للانطلاق وتوجد العديد من الفُرص لتعزيز وتحسين عملية التصويت باستخدام ICT سواءًا كانت داخل مراكز الاقتراع أو في حالة التصويت الإلكتروني عن بُعد للمُغتربين.

معتز: اليوم، يوجد العديد من حوادث الاختراق في مصر وتاشرق الأوسط، لماذا لا يكون لدينا مسابقة للمجتمع الآمني لتحدي مهارات المتخصصين وتشجيعهم على التوجه إلى مجتمع القبعة البيضاء بدلاً من التوجه إلى السوداء خصوصًا بالنسبة للمراهقين؟

د/ شريف: فكرة عظيمة! أنا أقترح أن تقوم أنت بالمبادرة، وتدع لنا معرفة كيفية دعم هذه المبادرة.

معتز: ما هو رأيك في مجلة سيكيورتي كايزن وفي مبادرات مؤتمر القاهرة الآمني (CS Camp) خصوصًا بعد تقديم مسابقة "التقاط العلم" لأول مرة في مصر؟

د/ شريف: لقد استمتعت بالمؤتمر، على الأقل بالجزء الذي قمت بحضوره. ولقد أعجبتني أيضًا فكرة المسابقة. استمر بالعمل الجيد الذي تقوم به.

Best Practice

تأسيس وعي ناضج بأمن المعلومات والنماذج التعليمية

إن أمن المعلومات هو حماية المعلومات والأنظمة التي تدعمهم مباشرةً من الاستخدام أو الدخول أو الكشف أو التعطل أو التعديل أو التدمير غير المُصرح به. تقوم أي منظمة بغض النظر عن حجمها أو عددها باستخدام الآليات التالية لممارسة وتحسين أمن المعلومات لديهم. إن الآليات المُستخدمة هي الأشخاص والعمليات والتكنولوجيا.

شكل 1

إن العامل الوحيد المُشترك كما هو مُوضح من الشكل أعلاه أن الأشخاص هم من يقوم بإدارة العمليات والتكنولوجيا. ولذلك، فإن كل موظف دائم أو مؤقت أو متعهد أو شريك أو بائع..إلخ، لديه دوره ومسؤولياته في أمن المعلومات التي يحتاج إلى إتمامها. من هنا تأتي أهمية إيصال معلومات كافية ووافية لكل العاملين فيما يخُص المسؤوليات الأمنية. إن الوعي بأمن المعلومات شديد الأهمية لأي استراتيجية أمن خاصة بالمنظمات ودعم عمليات الأمن. وعلى الرغم من أهمية توعية المُستخدمين بدورهم ومسؤوليتهم في الأمن فإن ٪64 من المنظمات في أمريكا و٪48 من منظمات إنجلترا و٪59 من منظمات الهند فقط تقوم بتوفير برامج توعية أمنية على الرغم من اللوائح التي تأمر بذلك. والكثير من الحوادث الأمنية التي تؤدي إلى خسارة ملايين الدولارات كغرامات وخسارة السمعة التي كان من المُمكن تجنبها بتوفير وعي وتدريب أمني مُناسب. لا يُركز هذا البحث على المُستخدمين النهائيين فقط ولكن على المُستخدمين التقنيين وكبار المديرين الذين غالبًا ما ينسون ذلك.

ماهي القيم التي يقوم الوعي والتعليم الأمني بتوصيلها؟ إن وجود برامج تعليمية شاملة ومدروسة خاصة بأمن المعلومات سيؤدي إلى زيادة وتنظيم الأمن في المنظمة. لنرى في الجدول المخاطر التي تشمل عامل الأشخاص وإمكانية تفاديها ببرامج وعي حقيقية.
يوضح لنا الجدول أعلاه أن الوعي والتدريب الأمني يُعد شيئًا أساسيًا لكل أعضاء المنظمة. لنرى الآن كيفية إنشاء برنامج توعية أمن المعلومات.

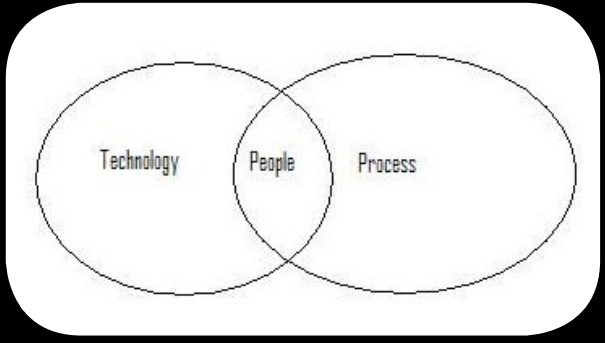


Figure 1

Risk Seed	Threats	Medium of threat	Impact
Human Resources	Social Engineering	Phones, Instant messengers, posits.box muffing	Loss of Customer intimacy.
Human Resources	Password disclosure	Risk Seed	Loss of reputation, financial penalties.
Human Resources	Insecure software coding leading to various vulnerabilities.	Internal development environment	Loss of CIA and can also lead to Financial impacts

أعمدة توعية وتعليم أمن المعلومات:
إن الأشخاص الصحيحين والتزام الإدارة وسياسات أمن المعلومات تُشكل الأعمدة لبرنامج فعال للتوعية وتعليم بأمن المعلومات

سياسات أمن المعلومات:
احصل على سياسات أمن معلومات مُنظمة ومُحدثة تُدعم رؤية ورسالة المنظمة. اجعلهم في مواجهة التهديدات الموجودة واجعل فريق تكنولوجيا المعلومات الداخلي يقوم بتقييمهم شهريًا. ثم قم بعرض التقييمات على الإدارة العُليا. ستضمن لك هذه الخطوات الحصول على سياسات مُحدثة وعرضها على الإدارة العُليا سيضمن لك دعمها.

التزام الإدارة:
تأكد من التزام الإدارة قبل أن تبدأ مثل هذه الخطة. فإن وجود برنامج وعي أمن معلوماتي شامل وناضج للمنظمة يُزيد وضع الأمن ووضع التواصل الداخلي في المنظمة أيضًا مما يساعد على زيادة الفعالية الوظيفية وتوفير مجتمع عمل صحي. واذكر تلك المُميزات للإدارة واحصل على موافقتهم. ويُعد الحصول على موافقة الإدارة تنشر إشارت إيجابية في المنظمة التي تلتزم الإدراة بتطويرها وإبقائها آمنة.

الأشخاص الصحيحين:
الأشخاص هم العامل الأول لنجاح أي منظمة. ووجود الأشخاص الصحيحين في أي فريق هو مايصنع الفرق من أجل عمل أي خطة أو استراتيجية ناجحة. حاول دائما أن تقوم بتوظيف الأشخاص بعد التأكد من خلفيتهم للوظائف التي لا تحتاج لخبرات سابقة. أما إذا كنت ستقوم بتوظيف شخصًا لوظيفة متوسطة أو عُليا فحاول أن تتأكد من كل إمكانياته مثل التعليم والوظائف السابقة والعمل الجماعي والمؤتمرات والمؤسسات وتاريخه الشخصي وتأكد أنه ملتزم في سعيه للتميز. ويؤدي هذا لخلق البيئة المناسبة لبناء الخطة.

تكوين فريق:
بعد اختيار الأشخاص المناسبين، يجب عليك أن تقوم بتشكيل لجنة أساسية تشمل وتضم أعضاء من أقسام الأعمال المختلفة. يُعد تكوين الفريق شيئًا أساسيًا للوصول إلى النجاح وسيتم مناقشته فيما بعد.

أعضاء اللجنة الأساسية:
يُفضل أن يكون أعضاء اللجنة الأساسية رؤساء الأعضاء من جميع أقسام الأعمال. وهذا هو ما سيضمن لهم دعمهم الذي يُعد مهمًا جدًا من أجل نجاح برنامج التوعية. ويجب أيضًا أن يكون مسؤول أمن المعلومات جزءًا من اللجنة الأساسية.

مجموعة أبطال التوعية الأمنية:
يجب أن يتم تكوين مجموعة أبطال التوعية الأمنية وأن يكون مُكون من رؤساء الأعضاء في العمل. الأشخاص المُنضمين للمجموعة يجب أن يملكوا المميزات التالية:

1. المعرفة بالعمل: الشخص المُختار كبطل توعية لابد أن يكون لديه معرفة سليمة بأساليب العمل. وهذا أمر مهم عند مقارنة المخاطر الأمنية بالعمليات والسياسات والاستراتيجيات الجديدة للمنظمة.
2. مُتخصص في مجاله: يجب أن يكون الشخص المُختار مُتخصص في مجاله. مما يضمن احترام أعضاء مجموعته وزملائه في العمل ويضمن تأمين النقطة الرابعة.
3. احترام الزملاء: يجب أن يكون الأشخاص المُختارين كأبطال توعية محترمين من قِبل زملائهم في أقسام عملهم. مما يضمن التزام مجموعته لأن شخصًا من هذه النوعية يسمعه ويحترمه أعضاء مجموعته.
4. مُحاور ناجح: يجب أن يملك الأشخاص مهارات اتصال كبيرة ومؤثرة، ويعرفون أكثر من لغة ويتحدثونها بطلاقة. مثلما يتحدث شخصًا ما اللغة الإنجليزية ويتحدث بطلاقة لغته الأصلية (اللغة العربية)، مما يضمن الاهتمام بالأشخاص المُتحدثين بلغات مختلفة في المنظمة.

المجموعة المُتخصصة بأمن المعلومات:
يجب أن تتكون هذه المجموعة من الأعضاء من مختلف الأقسام الذين يسعون للتميز وتطوير منظماتهم. يجب أن يكون مُتادًا لهم إمكانية ترقيتهم كأبطال توعية كجزء من التزامهم لتوعية أمن المعلومات.

مجموعة توعية تكنولوجيا المعلومات:
تهتم هذه المجموعة خصيصًا بقسم تكنولوجيا المعلومات. وتتضمن رؤساء أعضاء الأقسام ويتابع متطلبات التدريب التي يحتاجها الأشخاص في الأقسام. وتقوم المجموعة أيضًا بقياس مدى نجاح التدريب بمقاييس تكنولوجيا المعلومات.
تكوين الفريق وأعضاء الفريق يجب أن يتضمن الموارد البشرية وخدمة العملاء وتكنولوجيا المعلومات وأقسام أخرى، ويجب أن يحصل على موافقة 3\4 أعضاء اللجنة الأساسية. وفيما يلي شكل توضيحي للرجوع إليه (شكل 2)

تحديد الاحتياجات: لا يتساوى كل المُستخدمين. ستُحدد هذه المرحلة احتياجات التدريب لكل فرد حسب المسؤوليات التي يتحملونها. يتم تقييم احتياجات التدريب حسب المسؤوليات والنتائج التي من المُفترض الوصول إليها. يتم تحديد المسؤوليات حسب النظام والهدف واحتياجات التدريب. يُمكن استخدام طريقة بسيطة موضحة بالأسفل.

بما أننا نعمل بالقول أن المُستخدمين لا يتساوون، ويتم تقييم معرفة كل مُستخدم فيما يتعلق بالتوعية الأمنية والخبرة بالنظام والمعرفة بالحاسب الآلي بشكل فردي عن طريق استمارات تقييم قام أبطال توعية أمن المعلومات بتطويرها. ويجب تحضير الاستمارات الخاصة بتوعية أمن المعلومات مع مراعاة المُستخدم العادي والمستخدم المُتخصص. أما استمارات تقييم تكنولوجيا المعلومات فيجب أن تكون دورية لتقييم مُوظفي تكنولوجيا المعلومات ومعلوماتهم في مختلف المجالات. ومن الموصى به استخدام التقييمات على الإنترنت لسهولة جمعها وتعديلها. وسيُساعدنا هذا أيضًا على تحليل النقص وتحسين مستوى المعلومات للمُستخدمين. يُمكنك تحديد احتياجات التدريب ومستوى المعرفة لديهم حسب الإجابات والمقابلات الشخصية مع الأشخاص. ويُمكنك وضعهم في ملف بالشكل البسيط الموضح أدناه. إن الهدف الإساسي من نموذج التقرير هو تنظيم المقال وتوضيح الفكرة.

سنشرح بالتفصيل ما المقصود بأساسي ومتوسط ومُتقدم:
تدريب أساسي: للمُستخدمين الذين يُمكن أن يؤدي جهلهم إلى أقل تأثير على المنظمة ومواردها. وتُسبب هذه التأثيرات خسارة مالية قليلة ولا تُسبب أي خسارة للسمعة والنزاهة.
تدريب متوسط: للمُستخدمين الذين يُمكن أن يؤدي جهلهم إلى بعض الضرر للمنظمة ومواردها لكن لا يُسبب خسارة مالية كبيرة ولا يُسئ لسمعة المنظمة.

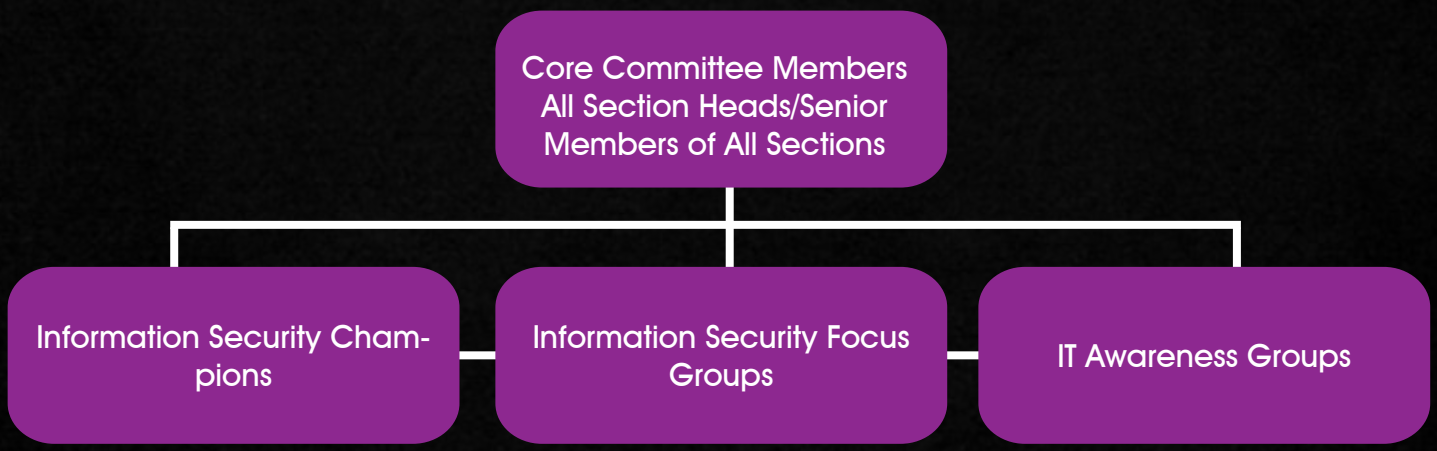
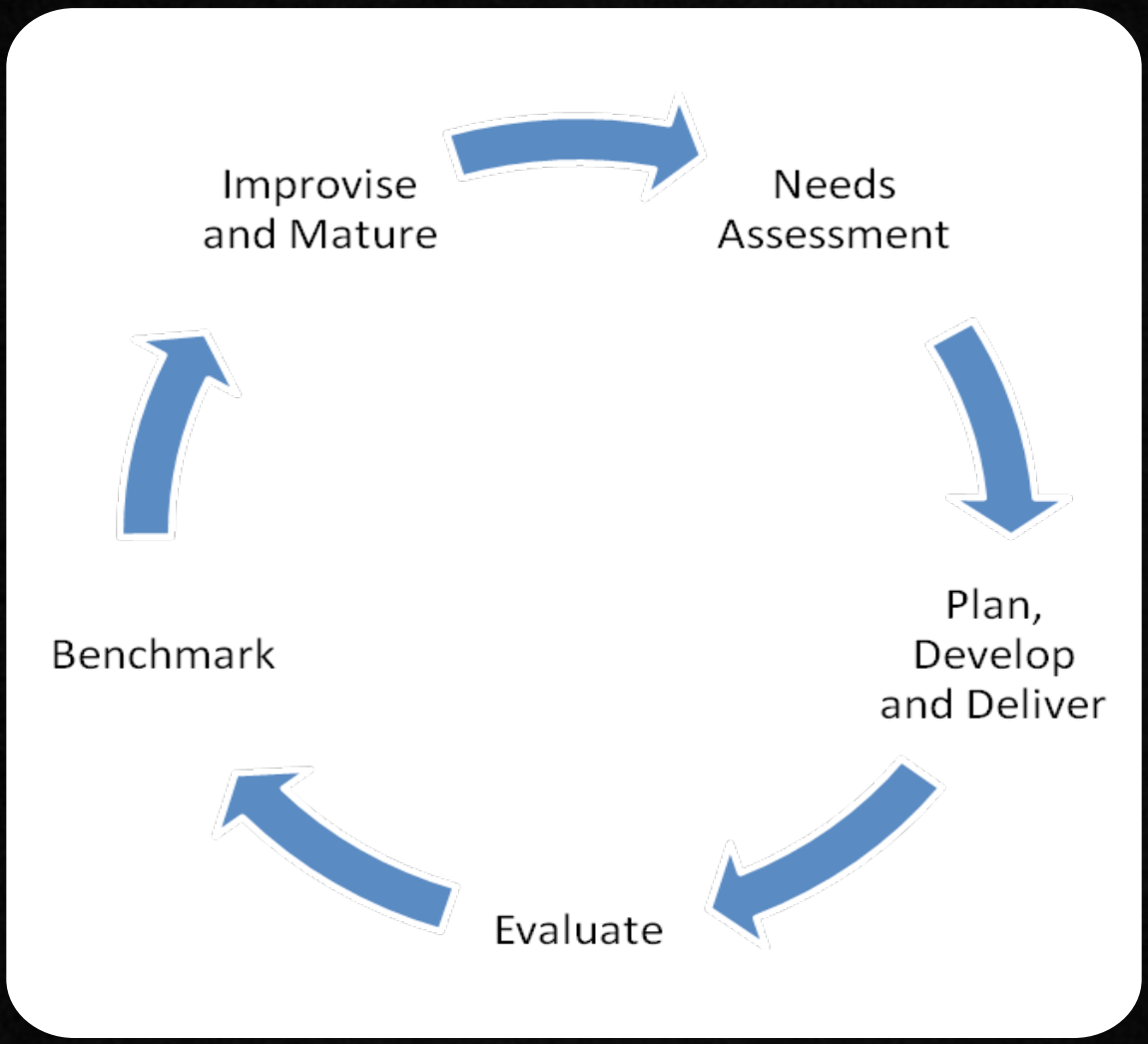


Figure 2



End user Security awareness Model: Figure 3

تدريب متقدم: للمُستخدمين الذين يُمكن أن يؤدي جهلهم لخسارة مالية كبيرة وتخريب السمعة ويؤدي إلى خسارة المصداقية والتقارب مع العميل.

طور ووصل: بعد القيام بتقييم الاحتياجات. قم بالتخطيط والتطوير وتوصيل الوعي الأمني والبرامج التعليمية في المنظمة. كل عملية موضحة بالتفصيل فيما يلي.

التطوير: هذه الخطوة تتضمن تجميع موارد التدريب المتاحة مثل الأشخاص والمحتوى وتطوير مواد التدريب. يجب أن يتم تطوير مواد التدريب بواسطة فريق أبطال الوعي الأمني والفريق المُتخصص بالوعي الأمني مع وضع النقاط التالية في الاعتبار.
ما هو رد الفعل الذي نُريد المُستخدم أن يقوم بها؟
ما المهارات التي نُريد أن يتعلمها المُستخدم ويقوم بتطبيقها؟
هل سيصل هذا المحتوى بسهولة؟
هناك الكثير من المواد المتاحة التي تتطلب نقلها إلى كل فرد في المؤسسة على حِدة حسب مسؤولياتهم ومستوى معلوماتهم المطلوب، هذا الموضوع أكبر من أن نستطيع مناقشته هنا. يجب أن يتأكد أبطال خدمة تكنولوجيا

Needs Assessment Report:

Employee ID	Responsi-bilities	System ex-posure	Impact	Training Needs	Knowledge Level
1234	Payroll Processing	Fair	Loss of Confiden-tiality and integrity	Basic	Advanced
5678	Solving cus-tomer related issues through Phone calls, Emails and Service desk system	Good	Loss of avail-ability, social engineer-ing that could lead to financial impacts and loss of repu-tation.	Advanced	Intermedi-ate
891	Floating purchase tenders	Fair	Poor quality equipments , leading to financial loss	Intermedi-ate	Basic

المعلومات بالمشاركة مع الفريق المُتخصص أن المناطق المهمة تم تغطيتها. والقيام بتصنيف المواضيع المطلوبة لكل مستوى.

بعد مراجعة التصميم والتخطيط، قم بتوصيل الخطة للمُستخدمين النهائيين طبقًا لاحتياجاتهم التدريبة التي تم تقييمها عبر مختلف الوسائل المتاحة في المؤسسة. يجب أن يتم تقييم خطة وطرق التدريب الخاصة بكلاً من اللجنة الأساسية وفريق أبطال التوعية والفريق المُتخصص. يجب أن تعطي الفرق المُتخصصة في أمن المعلومات المواضيع الأساسية والمتوسطة بينما يتم إيصال المواضيع المُقدمة إلى أبطال توعية أمن المعلومات من قسم تكنولوجيا المعلومات.

كن خلاقًا وقم بالتقييم:
بعد توصيل المحتوى، يجب أن يتم تقييم المُستخدمين في بيئة مُحكمة للتأكد من فهمهم للمواضيع بشكل جيد. ولا بد من تحضير نموذج تقرير ما بعد التقييم لترى ما إذا كنت قد حصلت على النتائج المرجُوة من التدريب. يجب أن يحصل المُقَيِّم على معلومات من المُرشحين لمعرفة مايجب تحسينه من المحتويات والعروض وغيرها. سيكون تجميع المعلومات سهلاً إذا كانت على الإنترنت وستصل إلى نتائج أفضل في المستقبل. ثم قم بتحديد أدائك الحالي وطوره باستمرار للحصول على نتائج أفضل.

يتم وضع تقرير ما بعد التقييم في مكان يُمكن لكل الفرق الوصول إليه. هذا سيضمن التطوير المستمر بشكل دوري. يُمكن لأبطال الأمن أيضًا تطوير نظام درجات القسم لمعرفة أفضل قسم في الأداء وتكريمه في النشرات

Training Needs	Topics	Delivery Method	Schedule/ Frequency	Audience
Training Needs	Review of Security policies and acceptance	Face to Face	New hires and Annual	Everybody
Basic	Laptop Security	Face to Face, Bulletins	Quarterly	Laptop users
Basic	Incident Management	Face to Face, Bulletins and handbooks	Bi Monthly	Help Desk Users

الداخلية الإخبارية. هذا بالتأكيد سيُحسن الصحة المؤسسية في مجال الأمن والأداء.
لا ينتهي تعليم أمن المعلومات عند المُستخدمين النهائيين كما تفعل معظم المؤسسات، قسم تكنولوجيا المعلومات أيضًا يحتاج إلى تعليمه باستمرار ليعرفوا آخر التطورات في الأنظمة والتهديدات الموجودة. كما هو موضح أعلاه.

حدد الثغرات: مسؤول أمن المعلومات ومدير تكنولوجيا المعلومات وموظفي أمن المعلومات يجب أن يقوموا بإجراء مراجعات دورية على الأشخاص في أقسامهم للتأكد أنهم يملكون المعلومات الكافية ليتعاملوا مع التهديدات الموجودة ومعرفتهم بالمعايير الجديدة والاتجاهات الحالية وغيرها. و تقييم الاحتياجات يتم مثل تقييم الاحتياجات كما هو موضح للمُستخدمين النهائيين.

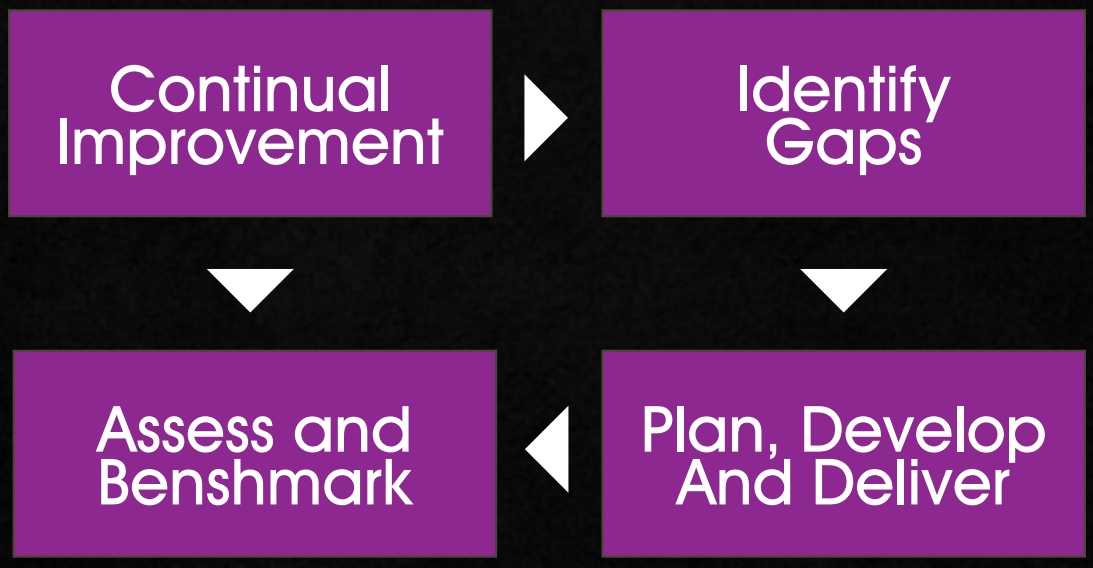
استثمر في المواد التعليمية:يجب أن تستثمر المنظمة وتحضر مواد تعليمية ذات جودة عالية مثل: ISSA وISACA وISC2 وIEEE وغيرهم. وبالاستثمار في مثل هذه المجلات والمواد ستضمن المنظمة زيادة المستوى العلمي للأشخاص في تكنولوجيا المعلومات مما سيؤدي إلى أكواد أفضل وتحسين العمليات، إلخ. هذه المجلات تُسهل الطريق لمعرفة تقييمات الاحتياجات الفعالة.

Presenter ID	Content	Delivery Method	Remarks of candidate
1234	5678	Webinar	Points can be split further which will help us comprehend better.
1234	5678	Face to Face and Webinar	Webinar was good but the presenter gave fewer examples in relation to password security.

Employee ID	Topics	Password policy	Performance Score	Performance and remarks
1234	Wireless Security	Webinar	60 percent	Average performance, need to have a one on one session to make him excel.
5678	Password policy	Face to Face and Webinar	80 percent	Optimum performance must educate the user through bulletins and targeted Email to help him Excel. Next examination to be conducted next month same date.

خطط وطور وقم بالتوصيل ثم التقييم والتحسين: بعد إجراء تقييم احتياجات يجب أن تقوم بالمراجعة لتعرف ما إذا كان الأشخاص داخل المنظمة مؤهلين لتغطية الثغرات أم لا. وإذا لم يكونوا مؤهلين فابدأ بتحضير المحتويات وطرق توصيل الخطط لتعليمهم. وفي بعض الحالات، يكون ضروريًا إحضار خبير خارجي لتدريب الأشخاص. وفي هذه الحالة، يُمكنك في حدود ميزانيتك تدريب كبار الأعضاء والفرق وإعادة تدريبهم ليدربوا بقية الأعضاء. وبهذه الطريقة يُمكنك نشر العلم في المنظمة. قم بحفظ التدريب وقَيّمهُم داخليًا وحافظ على تطويرهم باستمرار. يجب أن يتم إجراء احتياجات التعليم الأمني الذي يعتمد على تكنولوجيا المعلومات مرتين شهريًا من أجل جودة أفضل وللبقاء على إطلاع بالتهديدات المتطورة والأنظمة الجديدة.

ختامًا: إن الوعي والتعليم بأمن المعلومات متواصل ومستمر. بدعم إداري ملائم والأشخاص المناسبين وتكوين جيد للفريق وضم جميع أقسام الأعمال في العملية يُمكّننا من الحصول على التزامهم ما سيضمن وعي وتعليم أمني ناجح لكل فرد وللمنظمة التي تسعى للوعي والتعليم الأمني لزيادة الفعالية الوظيفية و الصحة المنظمية.



المراجع:

http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf
csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

Vinoth Sivasubramanian

الحاصل على شهادات CEH وABRCCIP وISO 27001 LA، لديه أكثر من 7 سنوات خبرة في مجال نظام أمن المعلومات

An up to date link with the security community bk news is your way

www.bluekaizen.org/bknews.php

أدوات تجربة التّخفيف المحسّنة (EMET)

تُهدد نقاط ضعف برامج الكمبيوتر وكشفها نظام معلومات المُستخدم وتجربته مع الكمبيوتر يوميًا. وعادةً ما تصبح بعض التطبيقات المشهورة هدفًا لهذه التهديدات مثل تطبيقات معالجة النصوص ومُشغلات الوسائط والمتصفح ويتم استخدام امتدادتهم للحصول على المنافع العديدة لتسهيل الإنتاجية المهنية والشخصية. المشكلة الأساسية تكمُن الطريقة التي تكشف بها نقاط الضعف بدون أي تفاعل من المُستخدم لأنه ببساطة يقوم بالتحميل والتفعيل ببساطة بواسطة زيارة موقع ضار أو تحميل ملف ضار. لا يملك المُستخدم العادي عادةً أي فكرة عن محتويات الموقع أو التطبيق الذي يتم استغلاله لتحميل البرامج الضارة لأغراض شريرة أو لنشرها لأنظمة اخرى.

نادرًا ما يقوم المُستخدم والشركات بتصحيح هذه المنتجات نظرًا لعوامل كثيرة مثل نقص الأدوات المتاحة وعمليات التأمين ضد البرامج السيئة أو غير المُكتملة وضعف الإدارة الأمنية وقلة ثقافة المنظمة. إن معدل هجمات يوم-الصفر (the zero day) لتطبيقات العملاء في زيادة طبقًا لشركات استخابرات نقاط الضعف على مستوى العالم منها تقارير IBM X-Force Threat. وطبقًا لتقرير SANSبعنوان"أخطر التهديدات الأمنية الإلكترونية" فإن البرامج التي لم يتم تأمينها عند العملاء هي أخطر التهديدات على الإطلاق. ومن المثير للدهشة والاحباط ملاحظة أن البائعين لم يقوموا بتأمين التطبيقات من نقاط ضعف يوم-الصفر على الرغم من الإعلان عنها منذ سنتين في تقرير SANS.

ومن المعروف أن حقيقة التوقيعات المُعتمدة على منتجات تكنولوجيا برامج كشف التجسس إزالتها تخسر الحرب لأنها لا تستطيع مجاراة البرامج الضارة المتنوعة والمُتجددة يوميًا. إن الحل الوحيد الذي يُعطي الأمل هو معالجة نقاط الضعف من داخل الأنظمة لمواجهة الهجمات المختلفة التي تستغل آليات أنظمة التشغيل الأساسية. وقد قامت شركة مايكروسوفت مؤخرًا بإطلاق"مجموعة أدوات تجربة التّخفيف المحسّنة (EMET)" النسخة 2.0.0.3 في نوفمبر 2010 لجميع عملائها وأنظمة تشغيل مراكز الخدمة منها Windows XP وWindows VISTA وWindows 7 وWin-

dows Server 2003 و2008. في بداية إطلاقه لم يكن EMET مدعمًا من مايكروسوفت. وعلى مستوى الشركات يُمكن تحميل EMET يدويًا أو بأداة توزيع ونشر البرامج.

يعتمد نجاح أداة التخفيف EMET حقًا على مدى قبول هذه الأداة في مجتمع المُستخدمين وفي اتساع انتشارها. وقد أجبر طلب دعم هذه الأداة شركة كايكروسوفت على القيام بدعم EMET. وكذلك فإن الحاجة الماسة للميزة التي تُساعد على نجاح هذه التكنولوجيا في شريحة سوق الشركات هي إدارة أداة EMET بواسطة سياسات المجموعة، والتي بدونها تكون فرص انتشار أداة EMET في سوق الشركات معتمة. وستكون أداة EMET طبقة أخرى من الدفاع في عمق الدفاع الاستراتيجي في المستقبل القريب للتخفيف أو في أسوأ الحالات لتأخير نجاح عمليات الاستغلال في الأنظمة المُستهدفة.

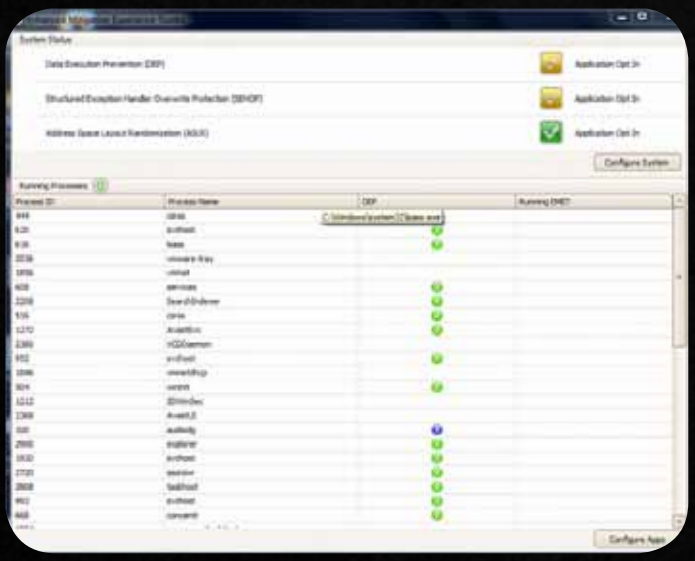
تبدو أداة EMET أنيقة حقًا، نظرًا للضوابط التي تقدمها لأساس المشاكل التي تواجهها أنظمة شركة مايكروسوفت الأساسية مثل ثغرات stack overflow وعشوائية العناوين.تعرض أداة EMETتقنيات تخفيف مثل حافظ البيانات DEP المُحمل تلقائيًا على IE8 وحافظ كتابة المعالجة الأستثنائية المنظمة (SEHOP) و-Heap Spray Alloca tion وNull Page Allocation وExport Address Allocation Table Access Filtering وMandatory Address Space Layout Randomization. كما تعرض مجموعةEMET مزايا أخرى متعددة. ولمزيد من التفاصيل عن أداة التخفيف وكيفية عملها أرجو مراجعة دليل مُستخدمEMET (ستجد الرابط أدنى المقال). وأوصي بوضع مُتصفحك على الإنترنت وAcrobat Reader وflash players في برنامجEMET لحمايتك من اختراق البرامج أثناء تصفحك المواقع الإلكترونية.

الأنظمة المُدعمة:
يدعم EMET 2.0 أنظمة التشغيل ومستويات حزم الخدمات الآتية:
أنظمة التشغيل الخاصة بالعملاء:

- Windows XP service packs 3 and above
- Windows Vista service pack 1 and above
- Windows 7 all service packs

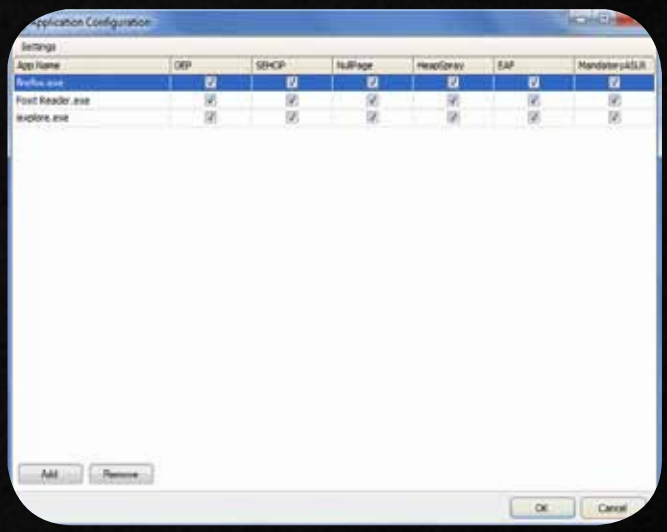
أنظمة التشغيل الخاصة بمراكز الخدمة:

- Windows Server 2003 service pack 1 and above
- Windows Server 2008 all service packs
- Windows Server 2008 R2 all service packs



تهيئة EMET:
يُمكنك العمل مع ميزة تهيئة أداة EMET بواسطة واجهة المُستخدم التخطيطية أو استخدام الأداة المساعدة بواسطة الأوامر.

بعد ان تقوم بتحميل أداةEMET ستحتاج لتحديد كمية الحماية التي تريد توفيرها. قم بالنقر على زر تهيئة النظام (configure system) كما هو موضح بشكل 1. ستظهر لك شاشة جديدة كما هو موضح بالشكل 2.
ضضغط بعدها علي زر تهيئة التطبيقات (con-figure application) وسيظهر لك الشكل 3. يُمكنك إضافة التطبيقات بالنقر على زر الإضافة مما سيحمي البرامج المُضافة. وأخيرًا قم بإعادة تشغيل الجهاز لكي يعمل البرنامج.



إن أداة EMET تُعد مُتحكم جيد في الأسباب الأساسية لنقاط الضعف في منتجات مايكروسوفت وتَعد بدفاع عميق المستوى لحماية نظم المعلومات. ومع القبول والطلب من المُستخدم لتطوير أداة EMET سنرى تطويرات أكبر لهذه الأدوات لتكاملها مع سياسات المجموعة. سيكون من الجيد رؤية الدعم الكامل لهذه الأدوات وإداراتها بواسطة سياسات المجموعة. وبالطبع لست في حاجة أن أقول أن هذه الأدوات في حاجة إلى أن يتم اختبارها لتوزيعها في بيئة إنتاجية لأنها قد تُعطل بعض التطبيقات الموجودة لذلك ستحتاج إلى اختبارات مكثفة قبل توزيعها. يُمكن أن يضيفEMET طبقة حماية جديدة لأعماق استراتيجات الدفاع.

المراجع

• IBM X-Force Threat Report - www-935.ibm.com/services/us/iss/xforce/trendreports
• Microsoft Security Report - www.microsoft.com/security/sir/default.aspx
• EMET mitigates Adobe Acrobat Reader exploit- www.itwire.com/business-it-news/security/41804-microsofts-emet-mitigates-adobe-acrobat-reader-attacks
• Here is the video from the EMET developers- http://technet.microsoft.com/en-us/security/ff859539.aspx
• EMET user guide - http://blogs.technet.com/cfs-filesystemfile.ashx/__key/CommunityServer-Components-PostAttachments/00-03-35-03-78/Users-Guide.pdf
• Some proof in support of EMET preventing exploits on IE 6,7 and 8- http://blogs.technet.com/b/srd/archive/2010/11/03/dep-emet-protect-against-attacks-on-the-latest-internet-explorer-vulnerability.aspx
• More proof of Acrobat reader zero day exploits being blocked from execution- http://www.ditii.com/2010/09/10/enhanced-mitigation-experience-emet-2-0-toolkit-blocks-adobe-reader-and-acrobat-zero-day-exploit/
• Download link in case you wish to try EMET on your lab or home devices - www.microsoft.com/downloads/en/details.aspx?FamilyID=c6f0a6ee-05ac-4eb6-acd0-362559fd2f04

Naveen Sharma

حاصل على شهادات CISSP وCISM وSANS GCIH وFCNSA. يعمل كمُقدم خدمات التقنية عالية المستوى في سيدني-استراليا. ويحب تحليل البرامج الضارة وتقنيات تأمين أنظمة الخدمات وتحليل الشبكات. ويقرأ الكثير عن أمن المعلومات.

مجلة
عرب هاردوير ™
ARABHARDWARE

مجلة تقنية شهرية للمبتدئين والمحترفين

- هاردوير
- سوفتوير
- العاب
- هواتف
- شركات ومؤسسات
- وغيرها من الأبواب الشيقة

الأن فى الأسواق

لمزيد من التفاصيل زورونا على :

http://magazine.arabhardware.net

Magazine المجلة

Cairo Security Summit

Cairo International Conference Center

26-29 APRIL

@ CAIRO ICT 2012

International Telecommunication, Information Technology
Trade Fair and Forum of The Middle East and North Africa

The Spring Of Technologies

From Dreams To Needs

MERCURY COMMUNICATIONS

Topics:

- **Track 1:** Mobile and Smart device Security
- **Track 2:** Vulnerability & Incident Management
- **Track 3:** Cloud & Database Security
- **Track 4:** Enterprise Security
- **Track 5:** Web 2.0 Security
- **Track 6:** Defensive Tools & Techniques
- **Track 7:** e-Commerce Security - Emerging trends and strategies
- **Track 8:** Hackers and security
- **Track 9:** Security of the National Broadband Network
- **Track 10:** Global Security Challenges

In Cooperation with: ASC Arab Security Consultants

Organized by TradeFairs INTERNATIONAL

24 Menouf St., off Orouba St., Heliopolis, Cairo, Egypt

Tel. : + 20 (2) 269 10792/3/4/5/6/7
Fax : + 20 (2) 241 59852

Join our group on "Cairo ICT 2011" معرض مصر الدولي للاتصالات

securitysummit@cairoict.com

www.cairoict.com

Are you prepared to handle Cyber Security Incidents?

(CSIH)

CERT® Certified Computer Security Incident Handler

First Half - 2012

Creating & Managing Computer Security Incident Response Teams (CCSIRT)*: Jan 29 - Feb 1	Information Security for Technical Staff (ISTS): Apr 1 - Apr 5
Information Security for Technical Staff (ISTS): Feb 19 - Feb 23	Creating & Managing Computer Security Incident Response Teams (CCSIRT)*: May 20 - May 23
Advanced Incident Handling (AIH): Mar 18 - Mar 22	Information Security for Technical Staff (ISTS): Jun 3 - Jun 7

First Half - 2012

*: Courses CCSIRT & MCSIRT must be booked together
All courses include 5 stars coffee break & lunch

Digital Risk Intelligence

SEI Partner | Carnegie Mellon

DRI page @ SEI:
www.sei.cmu.edu/partners/digitalrisk
Registration: www.digitalriskintelligence.com/register
info: training@digitalriskintelligence.com
Trainees should bring their laptops be able to run the labs

SPECIAL PRICES - CONTACT US

Rules of Usage:

* The Coupon is valid only from 1/1/2012 till 30/4/2012
* Coupon is valid only for one user
* The Coupon is valid only in the printed copy of security kaizen magazine not the online one
* You have to bring the coupon to the training center after cutting it from the magazine
* The Coupon is valid only in the following Authorized Training Center:
  1- Arab Security Consultants", Nasr City, 02-22732620,
  Register online (http://www.asc-egypt.com/ec-council-egypt/ec-council-course-registration.html)
  2- NEN (6october ,Nasr City ,Maa'di ,Mansoura ,Zagazig ,Assuit ,Suhag ,Ismailia ,Protsaid ,Arish) " Management Building : 6 October, Tel.:+20 (2) 3830 0048"