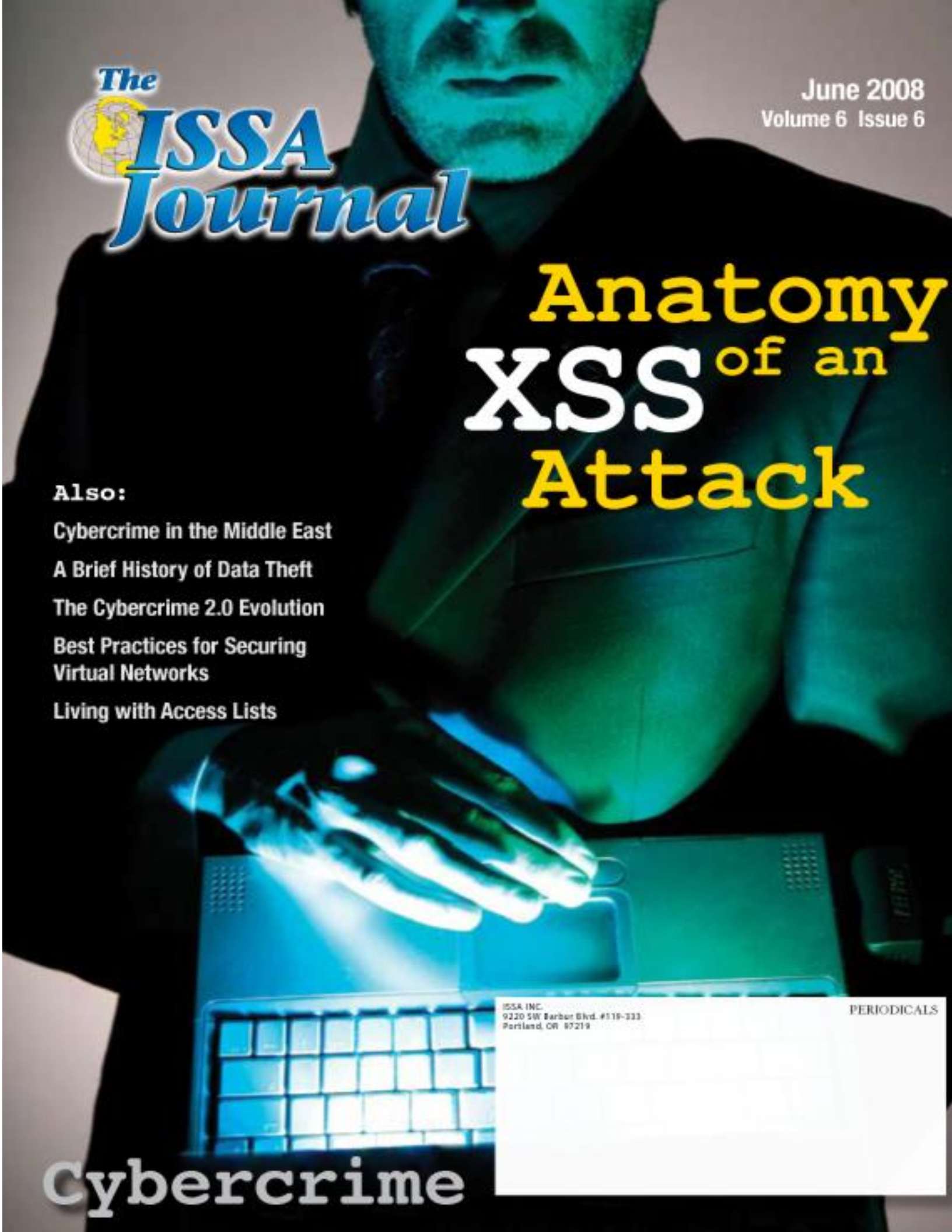

The ISSA Journal

June 2008
Volume 6 Issue 6

Anatomy of an XSS Attack

Also:

Cybercrime in the Middle East

A Brief History of Data Theft

The Cybercrime 2.0 Evolution

Best Practices for Securing Virtual Networks

Living with Access Lists

ISSA INC.
9220 SW Barbur Blvd. #119-333
Portland, OR 97219

PERIODICALS

Cybercrime

Cybercrime in the Middle East

الجريمة الإليكترونية في الشرق الأوسط

By Mohamed N. El-Guindy – ISSA Egypt Chapter President

اول نظرة موضوعية عن الجريمة الإليكترونية في الشرق الأوسط

بقلم: د. محمد الجندي / رئيس مجلس ادارة منظمة امن المعلومات / فرع مصر

المقال مترجم بتصريف من المقال الاصلي على موقع منظمة امن المعلومات وفى مجلة امن المعلومات طبعة يونيه 2008

الجريمة الإليكترونية ليست قاصرة على منطقة او دولة معينة ولكنها مشكلة عالمية.
إلا ان الشرق الاوسط قد شهد مؤخرا طفرة كبيرة في زيادة استخدام الإنترنت وزيادة في عدد المستخدمين لهذه الخدمة مما ادى بالتبعية إلى زيادة الجريمة الإليكترونية والتي تطلب تكثيف الجهود المبذوله لمحاربتها وايضا جهوضا كبيرة لتعزيز وتأمين البنية التحتية للمعلومات بالإضافة إلى نشر الوعي والتدريب للأفراد والمستخدمين وايضا تشريع قوانين تحكم الجريمة الإليكترونية او ما يطلق عليها Cyber Laws

قد لا تجد كلمة Cybercrime او الجريمة الإليكترونية في قاموس اللغة الإنجليزية إلا انه مصطلح شائع يصف الأعمال الإجرامية المتعلقة بالعالم اللإفتراضي او الإنترنت كما يطلق عليه Cyber Space وطبقا لتعريف المجلس الاوروبي فإن الجريمة الإليكترونية هي كل فعل اجرامي ضد شبكات الكمبيوتر او مستخدما شبكات الكمبيوتر يترتب عليه تهديد لعناصر امن المعلومات الثلاثة (توافرالمعلومة، سرية المعلومة، وسلامتها).

حالة أمن المعلومات في الشرق الأوسط State of Information Security

لكي نفهم لماذا الجريمة الإليكترونية في الشرق الاوسط مختلفة عن مثيلاتها في دول اخرى يجب ان نفهم حالة امن المعلومات في المنطقة وما العوامل التي تؤثر عليها من زيادة لعدد المستخدمين، نقص برامج التوعية بأمن المعلومات، عدم وجود تدريب كاف للجهات الأمنية

زيادة قاعدة المستخدمين للإنترنت في الشرق الأوسط
Growth of User Base

مع انتشار خدمات الإنترنت وانخفاض تكلفة الإشتراكات بدأت قاعدة المستخدمين في الزيادة بشكل ملحوظ مقارنة بدول العالم الأخرى فطبقا لإحصائيات الإنترنت العالمية Internet World States فان قاعدة المستخدمين زادت في الشرق الاوسط بمعدل 2.5% من حج الويادة العالمية للمستخدمين في ديسمبر 2007 . وايضا استخدام الإنترنت زاد في المنطقة بمعدل920.2% مقارنة ب 259.6% لبقية العالم في الفترة من 200 إلى 2007! وهذا العدد الكبير جدا من المستخدمين للإنترنت في المنطقة جعل الإنترنت اكثر شعبية ووسيلة مريحة للإتصال كما انها فتحت ابوابا جديدة للأعمال على الإنترنت. إلا ان اساءة الإستخدام زادت ايضا بسبب عدم وجود برامج توعية موجهة واصبح الكثيرون من مستخدمي الإنترنت في المنطقة ضحايا للإختراقات والجريمة الإليكترونية.

البنية التحتية للمعلومات. Information Infrastructure

الإستمارت في البينة التحتية للمعلومات كبيرة جدا في المنطقة وبخاصة دول الخليج إلا ان هناك الكثير من الخطوات يجب تطبيقها لسلامة هذه البينة التحتية اكثر من تركيبها او مجرد استخدامها. وفي المقابل ترى الكثير من المؤسسات وربما الهيئات الحكومية في المنطقة تخبرك بانهم لديهم اكثر الانظمة العالمية امانا وانهم مؤمنين ضد الإختراقات. إلا ان خبراء الإقتصاد في الشرق الاوسط يؤكدون ان البنوك وحدها في السنوات السابقة قد خسرت ما يقرب من بليون دولار من جراء الجريمة المنظمة والمعاملات الغير حقيقية والمزورة. وفي نفس الوقت لابد من الإشارة إلى ان معظم البنوك في المنطقة العربية تعاني من ما يسمى Phishing Attack او هجوم اصطياد المعلومات وهو ادعى لتوجيه المزيد من الإستثمارت في التوعية بأمن المعلومات.

أدت الإستثمارت في بنية المعلومات إلى زيادة الأهمية للتجارة الإليكترونية وايضا ما يسمة بالحكومات الإليكترونية e-Governments وايضا فتحت الفرص امام الأعمال الصغيرة في المنطقة مساعدة في ذلك في مشكلة البطالة. على الرغم من ذلك فأن الاسثمارت لتأسيس البنية التحتية لم ترعى اهتماما كبيرا لتأمين هذه البنية المعلوماتية. او كما تقول المقولة (العمل اولا، تأمينه في المرحلة التالية!) وايضا مزودي خدمة الإنترنت لم يضعوا تأمين البنية التحتية في حساباتهم بشكل كبير حيث اصبحت مشكلة عامة في المنطقة (العمل الأولى، تأمينه لاحقا)

على سبيل المثال بدون سيسات امنية متبعة من قبل مزودي الخدمة لحماية اعمالهم اصبح اكثر مزودي الخدمة في المنطقة محجوبون او Blacklisted بسبب الـ Spam او الرسائل المزعجة حيث يعتبر مزودي الخدمة في المنطقة من اكثر المصادر للـ Spam . الأمر يعتمد اكثر على

تكوين ثقافة امنية للمعلومات اكثر منه نظام امني او برنامج. فحتى اكثر البلدان العربية ثراءا ليست ببعيدة عن الجريمة الإليكترونية على سبيل المثال تم اختراق مواقع الحكومة الاماراتية من قبل محترفين وبقيت مخترقة لفترة مما ادى إلى خسائر مادية ومعنوية وايضا اتاحة معلومات سرية للعامة! اختراق موقع قناة الجزية من احد ابرز الامثلة ايضا على تعرض اسماء كبيرة في المنطقة للإختراق.

برامج توعية امنية فقيرة Poor Security Awareness Programs

برامج التوعية بأمن المعلومات من اكثر الطرق فعالية في محاربة الجريمة الإليكترونية فهناك نقص شديد جدا في برامج التوعية بامن المعلوت على مستوى الافراد والمؤسسات والحكومات مقارنة بالدول الاخرى مثل اوروبا والولايات المتحدة فالجهود في الشرق الاوسط ضئيلة جدا.

واحد اهم عوامل فشل او عدم فعالية برامج التوعية بأمن المعلومات المتاحة في المنطقة ان وجدت هي ان هذه البرامج متوفرة باللغة الانجليزية مما يجعل المهمة اصعب في توصيل الرسالة التوعوية للمتلقي لان ما يمكن تطبيقه في الولايات المتحدة مثلا يصعب تطبيقه بنفس الشكل في الدول العربية لوجود حاجز اللغة ولان هذه البرامج لا تتناسب مع طبيعة التفكير والثقافة في المنطقة.

غياب برامج التوعية بامن المعلومات هي ايضا مشكلة كبيرة في الشركات العاملة في تكنولوجيا المعلومات فمعظمهم ليسوا على دراية بالجريمة الإليكترونية ولا يعيرونها اهتماما واهمين ان الشرق الاوسط بعيد هذه المشكلة وانهم امنين. وفي النفس الوقت ليس لديهم سياسات امنية جيدة في امن المعلومات (نفس الشيء، العمل اولا، تأمينه لاحقا!)

على سبيل المثال صندوق بريد اليكتروني لموظف سابق في شركة كبرة وهذا البريد مازال فعال ولم يتم الغاؤه من قبل مدير الشبكة سوف يكون احد ادوات الحاق الضرر بالشركة من هذا الموظف السابق في اي لحظة وقد تسهل له الدخول غير المشروع للشبكة لسرقة بيانات مهمة قد تستخدم ضد الشركة فيما بعد!

فقر برامج التوعية لأمن المعلومات تعني ان الإنفاق على أمن المعلومات ضئيل جدا في المنطقة وايضا جهود محاربة الجريمة الاليكترونية ضئيلة جدا تاركة الأعمال في الشرق الاوسط عرضة للإختراقات. منطقة الشرق الاوسط في حاجة إلى برامج توعية وتدريب قوية جدا تستهدف الناطقين باللغة العربية لتدريب المستخدمين، العاملين في الشركات، رجال القانوين لفهم المشكلة وتداركها سريعا لان الامر يتفاقم يوما بعد يوم.

الشرق الأوسط كهدف للمجرمين على الإنترنت

A target for cybercriminals

حذرت العديد من المصادر ان الشرق الأوسط اصبح احد اكبر مصادر الجريمة الاليكترونية في العالم على سبيل المثال صنفت السعودية على انها اكبر مصدر وهدف في نفس الوقت لاعمال اجرامية عديدة على الإنترنت في منطقة الشرق الاوسط كما صنفت رقم 38 على مستوى العالم!

اما مصر فهي من اكثر البلدان التي تنتشر فيها هجمات Phishing في العالم طبقا لتقرير شركة Symantec تليها بعض دول الخليج مثل السعودية والأمارات وقطر وليس غريبا ان ترى انتشار الجريمة الاليكترونية في الشرق الاوسط في ظل غياب برامج توعية متخصصة تستهدف الشرائح المختلفة مع غياب التشريعات الخاصة بضبط هذه الجريمة. حتى الجريمة الالكيترونية العادية مثل Phishing او اصطياد المعلومات لها ايضا صفات مميزة في المنطقة قد تختلف عن مثيلاتها في اي دولة اخرى نظرا للوازع الديني المنتشر في المنطقة والمشكلات السياسية الكبرى. ويستخدم بعض الهاكرز هذه النقاط للحصول على معلومات من الضحايا قد تستغل ضدهم فيما بعد فقد يرسل الهاكر رسالة دينية او سياسة تحوي فيروس او برنامج تجسس وبالتالي سوف تلاقي ترحيبا من الكثيرين لفتحها والتعامل معها! ولك ان تتخيل ان يكون هذا الشخص الذي فتح الرسالة في بنك او في مؤسسة حكومية او اي شركة ففي هذه الحالة قد سهل عملية اختراق الشبكة الداخيلة للجهة دون ان يدري! ومن احد اكثر الاسباب ايضا التي ادت إلى انتشار الجريمة الاليكترونية في منطقة الخليج تحديدا هي انتشار المؤسسات المصرفية العالمية في المنطقة فأصبحت هدفا بالتأكيد في منطقة يغيب فيها الوعي الامني للمعلومات بالإضافة إلى مشكلات غسيل الاموال. وبما ان هذه الجهات المصرفية قد تستخدم تقنيات الإنترنت في التعامل مع الحسابات المصرفية والعملاء فانه ادعى ان تجد الكثير من النصب والإحتيال والهجوم ضد هذه المؤسسات في المنطقة. اضف إلى ذلك ان مشكلة غسيل الاموال قد ضاعفت من حجم البريد الخادع Scam الذي يتم ارساله للعديد من الضحايا في المنطقة لايهامهم بان هناك مبلغا من المال يراد تحويله من الإمارات مثلا إلى بلد اخرى في المنطقة وبالـاكيد نظرا لغياب التوعية فسوف يتفاعل الكثيرون مع هذه الرسالة والعواقب معرفة قد تنتهي بسرقة اموالك.

شبكات التعارف الإجتماعية Social Networking

بالطبع تكثر الجريمة الاليكترونية على المواقع التي تعج بالمستخدمين والأعضاء ولهذا فان مواقع التجمعات من اكثر المواقع جذبا للهاكرز والمتطفلين ومجرمي الإنترنت. واثبتت دراسات عديدة ان استخدام هذه المواقع قد يفتح ثغرات لا يحمد عقباها داخل شبكات الشركات والجهات الحكومية وحتى اختراق اجهزة العامة. ويبحث دائما الهاكرز عن المواقع التي تحوي عددا هائلا من المستخدمين والاعضاء والزوار وتفتقر غلى التوعية بامن المعلومات وليس هناك افضل من مواقع التجمعات. يحوي الشرق الاوسط اكثر من 27 موقع متخصص للتجمعات على الإنترنت والتي قد تستخدم من قبل الهاكرز لإصابة اجهزة المستخدمين ببرمجيات ضارة Malware مثل الفيروسات واحصنة طروادة او حتى تحويل المستخدم إلى موقع آخر لسرقة بياناته الخاصة وكلمة المرور وارقام الحسابات والفيزا وفتح ثغرات في اجهزة المستخدمين قد يستغلها الهاكر فيما بعد للحصول على معلومات من الضحية. وللأسف الشديد فإن مواقع التجمعات العربية لا تقدم الكثير من الأمن للمستخدمين سواء لمعلوماتهم الشخصية او لخصوصيتهم ولهذا نسمع يوميا عن جرائم ترتكب على الإنترنت باستخدام هذه المواقع. وتنتشر ايضا في الشرق الاوسط مواقع التجمعات العالمية مثل Facebook و Myspace وتستخدم في التعارف والصداقة وتكوين علاقات مختلفة وايضا التدوين والمدونات ورغم ان هذه المواقع لديها الكثير من امن المعلومات إلا ان استخدامها من قبل اشخاص لا يتمتعون بثقافة امن المعلومات وليس لديهم الوعي الكافي قد تؤدي إلى الكثير من الجرائم الاليكترونية ايضا مثل سرقة الهوية والكثير من الافعال الإجارمية على المستوى الشخصي او العام في شركة او منزل لا فرق! والمشكلة حقيقة متفاقمة وكبيرة ليس فقط في مواقع التجمعات ولكن ايضا في مواقع Web 2.0 المختلفة والتي تعطي الكثير من التفاعل مع الزوار مثل Blogs والدردشة Chatting والمنتديات والتي يمكن استغلالها من قبل الهاكرز طالما انه لا توجد توعية. وهذا ادعى إلى عمل برامج توعية متخصصة في المنطقة.

مشكلة البطالة Unemployment

تعاني اغلب بلدان الشرق الاوسط من مشكلة البطالة والارقام بالطبع تتزايد يوما عن يوم وهذا بدورة يؤثر في زيادة الجريمة الاليكترونية إذا لم تؤخ في الحسبان.

طبقا لتقرير البنك الدولي لإان الشرق الاوسط وشمال افريقيا لديهم تحدي كبير مع مشكلة البطالة إذ انه يتطلب عليهم توفير اكثر من 100 مليون وظيفة بحلول عام 2020 وإلا فان استقرار المنطقة سوف يتأثر بشكل كبير. وتشير الإحصائيات ان مشكلة البطالة تنتشر في الشباب اكثر من اية فئة اخرى واغلبهم بالطبع من خريجي الجامعات الذين يتمتعون ولو بقدر ضئيل من اساسيات استخدام الكمبيوتر والإنترنت وإذا لم يكن لديهم انترنت في المنزل فهم يلجؤن إلى مقاهي الإنترنت Cybercafes والتي تنتشر بشكل كبير في كل دول المنطقة وكل هذه العوامل تتكاتف بشكل ملحزظ لزيادة الجريمة الاليكترونية في المنطقة وخلق ما يسمى مجرمي الإنترنت المحليين اي من داخل المنطقة نفسها وليس من خارجها. ولكن اغلب هؤلاء سوف يكونون من يطلق عليهم Script Kiddies وهم اناس ليس لديهم الخبرة الكبيرة لبرمجة ادوات الإختراق بشكل احترافي ولكنهم قد يجيدون استخدام ادوات احترافية تم ابتكارها من قبل هاكرز محترفون وللأسف هؤلاء يمثلون الخطر الأكبر في المنطقة فلديهم الوقت الكبير ومنهم من لديه الدافع الديني ومنهم من يعمل للدافع المادي. ومع انتشار المواقع العربية التي تقدم خمات تعليم الإختراق وتحوي برامج مجانية للإختراق مع وصلات لمواقع اجنبية غير قانونية فالخطر اكبر بكثير مما نتخيل.

القوانين: ان وجدت فهي فقيرة جدا Regulations: Poor or None

معظم البلدان في المنطقة ليس لديها قوانين متخصصة في الجريمة الإليكترونية والقليل من البلدان تحاول سن تشريعات لهذا النوع من الجرائم مثل الإمارات والسعودية إلا انها مازالت في مراحلها الاولى وتحتاج إلى المزيد من التحسينات والتنقيح. وبسبب المشكلات السياسية في المنطقة فان معظم الدول تلجأ إلى استخدام ما يعرف بقوانين الطواريء Emergency Laws عوضا عن قوانين متخصصة للجريمة الاليكترونية كاسلوب من اساليب الردع للجريمة الاليكترونية على سبيل المثال القبض على المدونين بتهم السب والقذف وغيرها وبعض الدول الاخرى تلجأ إلى حجب المواقع التي يمكن ان تحدث عليها اي نوع من الجرائم الإليكترونية وكلا الحالتين بالطبع ليسا فعالتين على الإطلاق في محاربة الجرائم الاليكترونية وليس هناك اي تعريف واضح في القوانين المتاحة حاليا للجريمة الاليكترونية مما يؤدي إلى وضع مواطنين عاديين غير مذنبين وراء القضبان بتهم تتعلق بالجريمة الاليكترونية ولكنها في الحقيقة ليست كذلك لان الجريمة التي تستخدم الإنترنت تختلف اختلافا كليا من الناحية القانونية عن الجريمة التي تعتمد على الإنترنت!

وعدم وجود قوانين متخصصة بالتبعية تدل على عدم معرفة او وعي من الجهات المنفذة للقانون في المنطقة في ظل غياب التدريب والادوات التي تستخدم لمكافحة الجريمة الاليكترونية او حتى التحقيق فيها.

يعاني الشرق الاوسط من فقر في القوانين التي تحكم الملكية الفكرية والتعدي عليها باستخدام التقنيات الحديثة مثل الإنترنت. وطبقا لتقرير شركة Symantec فأن مصر تعد من اولى الدول اصابة بالفيروسات في الشرق الاوسط وهذا بالتبعية يعطينا مدلولا بان مصر ايضا تعد الاولى في انتهاك حقوق الملكية الفكرية وقرصنة البرامج لان الفيروسات تنتقل عبر الملفات التنفيذية وفي البرمجيات المقرصنة عبر شبكات Peer-to-Peer .

الدوافع وراء الجريمة الاليكترونية – Motivations for Cybercrime

الجريمة الاليكترونية في الشرق الاوسط لها دافعيين اساسيين هما الدافع المادي نظرا للمشاكل الإقتصادية والدافع الإرهابي نظرا لوجود التعصب الديني وما يتعلق به.

الدافع المادي – Financial

نظرا لمشكلة البطالة والتي اشرنا اليها فيما سبق وغياب التوعية بامن المعلومات في المنطقة ومع غياب القوانين فاصبح المجرمون يفكرون في طرق جديدة للإحتيال والنصب عبر الإنترنت ومع انتشار الـ Script Kiddies والمواقع التي تقوم بتعليم طرق الاحتيال والاختراق باللغة العربية اصبح الامر اكثر انتشارا وتعد مشكلة الـ Spam و Phishing من اكثر المشكلات تفاقما في الشرق الاوسط. ويستهدف المجرمون المحليون المستخدمين في منازلهم، مواقع التجارة الإليكترونية، البنوك والشركات المصرفية وشركات الاعمال الصغيرة نظرا لانعدام الوعي. وتتضمن الجريمة الاليكترونية بغرض الكسب المادي في المنطقة مسألة الملكية الفكرية وبيع البرامج المقرصنة والكثير من المنتجات التي يحرم القانون تداولها في المنطقة مثل المخدرات والجنس والدعارة. وقد تستخدم حملات الـ Spam او البريد الزائف لتوليد عدد زوار كبير على موقع معين بغرض سرقة اموال من شركة اعلانات معينة والتي بدورها تدرك المشكلة وتبدأ بحجب الزوار من منطقة الشرق الاوسط مما يؤدي إلى خسائر كبيرة لمن يقومون باعمال قانونية للربح من الإنترنت وايضا يشتهر الشرق الاوسط باكبر السرقات لكروت الفيزا والدفع على الإنترنت مما ادى إلى حجب اغلب بدان الشرق الاوسط من التعامل على بعض مواقع المعاملات الاليكترونية الشهيرة مثل PayPal.

الدافع الإرهابي – Terrorist

يلعب الدافع الارهابي دورا دراميا في الجريمة الاليكترونية في الشرق الاوسط ولعله الموضوع الاكثر اختلافا عن مثيله في اي منطقة اخرى حول العالم. وتستخدم الإنترنت في المنطة من قبل الجماعات الارهابية كوسيلة فعالة للإتصال وايضا وسيلة للهجوم على الاعداء. ولعل مشكلة الصراع الفلسطيني الاسرائيلي ومشكلة البطالة والمشاكل السياسة مجتمعة تؤدي إلى زيادة ما يعرف بالارهاب الإليكتروني والذي اخذ شكلا آخر في غسل عقول بعض المستخدمين ونشأ ما يعرف باسم (الجهاد على الإنترنت) Jihad Online والذين يعلنون انهم يستخدمون تقنيات الإختراق لمهاجمة الاعداء. ويستخدم الارهابيون مواقعهم كأٓلة فعالة للدعاية لافعالهم وايضا استقطاب اخرون للمساندة والاشتراك وايضا تستخدم المواقع في جمع التبرعات باسم الجهاد وايضا الحصول على معلومات من المستخدمين والاعضاء. وتقوم بعض مواقع الجهاد على الإنترنت بتجميع معلومات عن زوار معينين حسب اهتماماتهم وتخصصاتهم وقد تستقطبهم للعمل معهم فهي اداة جيدة للتعزيز وجمع البشر. ودائما يبحث اصحاب هذه المواقع عن المواهب الشابة التي تساعدهم في ادارة الموقع واستخدام التقنيات الحديثة ويتم استقطابهم بداية باسم الوازع الديني والذي يتحول فيما بعد باساليب مختلفة إلى دافع ارهابي! وليس بالطبع كل ما هو ديني فهو ارهابي ولكن نظرا لوجود الوازع الديني لدي الكثيرين في المنطقة لإان استقطابهم من قبل هذه المواقع وتغيير افكارهم لهو من الاعمال السهلة. ولا تستخدم المواقع فقط للتعرف على كيفية صنع القنابل والمتفجرات وانما تستخدم ايضا في الإعداد والتخطيط للهجمات التي تحدث في ارض الواقع وقد يستخدمون اساليب تشفير متطورة لأخفاء المعلومات عن بعض الجهات التي تراقب هذه المواقع.

الخاتمة – Conclusion

الجريمة الاليكترونية في الشرق الاوسط لها اثرها العالمي وبخاصة الجرائم الارهابية وعلى الرغم من الجهود التي تبذل الآن من قبل بعض الدول في المنطقة إلا ان الغالبية مازالت تعتمد على قوانين ليست مخصصة لهذا النوع من الجرائم. فلابد ان يكون سن تشريعات لمحاربة هذه الجرائم هو الهدف الاول للحكومات في المنطقة ويجب ان تتعلم بلداننا من الآخرون. هناك تجارب عديدة حول العالم ولكنها تحتاج إلى ما يسمى بالتوطين لكي تتوافق مع مجتمعاتنا. لابد ان نكون مستعدون لنوع جديد من الجريمة آخذ في الأزدياد يوميا لانها لاتؤثر على منظومتنا فقط ولكنها تطول الآخرين وتؤثر على علاقتنا بالأخرين حول العالم.

لهذا لابد من عمل برامج توعية مكثفة وقوية تستهدف المستخدمين في الشرق الاوسط من قبل الشركات والحكومات لتقليل هذه المخاطر ولابد من ضخ استثمارات اكبر في في تأمين وتعزيز البنية التحتية للمعلومات في المنطقة وايضا تدريب الجهات الحكومية والقانونية على آخر مستجدات امن المعلومات لان منطقتنا مليئة بالمشكلات بداية من مشكلات اقتصادية ومشكلات سياسية وكل هذه العوامل سوف تزيد من الجريمة الاليكترونية في المنطقة. ولكل من يظنون ان المنطقة بعيدة عن هذا النوع من الجرائم، لابد ان يدركوا اننا نعيش في عالم متصل ببعضه البعض.

ولا يهم اين تعيش او ماذا تفعل فسوف تتأثر بهذا الامر ان عاجلا او آجلا!

لذلك دعونا نتوقف عن مشاهدة ما يحدث حولنا ولنتحرك الآن (الأمن اولا)

عن المؤلف – About the Author

محمد نجيب الجندي
خبير في تكنولوجيا المعلومات لسنوات عديدة،

دكتوراه في تكنولوجيا المعلومات من جامعة كاليفورنيا بالولايات المتحدة
عضو في منظمة الكمبيوتر البريطانية BCS
خبير في تكنولوجيا المعلومات معتمد من المنظمة البريطانية لعلوم الكمبيوتر BCS CITP
عضو في معهد الهندسة والمهندسين بالولايات المتحدة IEEE
عضو في الجمعية العالمية للتعليم عن بعد بالولايات المتحدة WAOE
مدرج في قائمة (مشاهير العالم) Who is Who in the World
متحدث باسم ميكروسوفت

رئيس مجلس ادارة منظمة امن المعلومات فرع مصر ISSA-Egypt
مؤسس شركة ASK PC بالولايات المتحدة ومصر
مؤلف اول منهج متخصص في امن المعلومات باللغة العربية ومسجل في مكتبة الكونجرس