معلومات عامة
عن الاتحاد الدولي للاتصالات

الاتحاد الدولي للاتصالات: بناء الثقة في تكنولوجيا المعلومات والاتصالات والفضاء السيبراني

ويسر هذا البرنامج جهود الاتحاد لبناء القدرة التقنية الضرورية لمساعدة البلدان على مجابهة التهديدات السيبرانية، والتوصية بمعايير دولية بشأن الأمن والتكنولوجيا السيبرانيين، والعمل كمحفل للمناقشات حول المعارف والسياسات العامة.

وفقاً لتوقعات الاتحاد الدولي للاتصالات فإن عدد مستخدمي شبكة الإنترنت سيصل إلى نحو ثلاثة مليارات شخص قبل نهاية عام 2014، مما يفتح الباب أمام إمكانيات جديدة ومثيرة للوصول إلى المعلومات والاتصالات. على أن الشواغل ونقاط الضعف الأمنية في الشبكات والخدمات في الوقت ذاته تعرّض المستخدمين في كل مكان إلى تهديدات سيبرانية متزايدة التعقيد. ويمكن لعمليات انتحال الهوية الشخصية، والرسائل الاقتحامية، والبرمجيات الخبيثة، واستغلال الأطفال والمجموعات الأخرى المعرضة للخطر وإلحاق الأذى بهم، أن تخلّف جميعاً عواقب قاسية بل ومدمرة أحياناً في العالم الحقيقي تتجاوز نطاق الخسائر السنوية اللاحقة بالاقتصاد العالمي والمقدرة بنحو 400 مليار دولار أمريكي.[1]

وبما أن تكنولوجيا المعلومات والاتصالات (ICT) قد غدت بنية تحتية وطنية حاسمة فإن أي إخلال بها يمكن أن يؤدي إلى انقطاع كارثي في الخدمات الأساسية. وفي ظل بيئة تكنولوجيا النطاق العريض العاملة بشكل متواصل في أي زمان ومكان فإن الهجمات يمكن أن تُشن في بلد واحد، بل وحتى في عدة بلدان في آن معاً، في حين يكون مرتكبها موجوداً في مكان لا علاقة له مطلقاً بالبلدان المعنية.

غدت التهديدات السيبرانية خطراً يحدق بكل بلد، حتى البلدان الأكثر تقدماً من الزاوية التقنية. ويمكن لتعزيز التعاون الدولي أن يخفف من وطأة هذا الخطر.

خطر دولي متصاعد

- وصل عدد ضحايا التهديدات السيبرانية عام 2013 إلى نحو 400 مليون ضحية.
- شهد عام 2013 زيادة بنسبة 91% في الحملات الهجومية الموجهة. وزاد عدد الخروقات بنسبة 62%، وعانت نسبة 38% من مستخدمي الخدمات المتنقلة من الجريمة السيبرانية.
- قفز عدد 'الهويات الشخصية المعرضة للخطر' بشدة بمعدل يزيد على خمسة أمثال عام 2013 بحيث وصل إلى 552 مليون هوية بالمقارنة مع 93 مليون هوية عام 2012.
- إن القطاعات الثلاثة الأولى المعرضة لخطر الهجمات الموجهة هي القطاع الحكومي، وقطاع التعدين، وقطاع التصنيع (شركة Symantec، تقرير التهديدات الأمنية في شبكة الإنترنت).

ويقوم مستخدمو الخدمات المتنقلة بتخزين الملفات الحساسة على الخط (52%)، كما يخزنون عملهم ومعلوماتهم الشخصية في حسابات التخزين على الخط ذاتها (24%)، وكثيراً ما يقومون بتخزين معلومات تسجيل الدخول وكلمات المرور مع أسرهم (21%) وأصدقائهم (18%)، بحيث يعرضون للخطر بياناتهم وبيانات أصحاب عملهم. وتبلغ نسبة المستخدمين الذين يكتفون باتخاذ الاحتياطات الأمنية الأساسية لا غير، 50% فحسب وفقاً لشركة Symantec المندرجة في عداد شركاء الاتحاد الدولي للاتصالات.

1. McAfee

اطلعوا على مزيد من المعلومات عن أنشطة الاتحاد الدولي للاتصالات في مدونة الاتحاد الإلكترونية:
http://itu4u.wordpress.com

هذه إحاطة بمعلومات أساسية الغرض منها تيسير عمل وسائل الإعلام وينبغي ألا تُعتبر معلومات شاملة ولا أن تُعتبر بياناً رسمياً عن أنشطة الاتحاد.

ومع تحول 'إنترنت الأشياء' إلى حقيقة واقعة، وقيام ملايين الأجهزة المترابطة بتبادل المعلومات من آلة إلى أخرى دون الحاجة إلى تدخل بشري فإن عالمنا المادي والعالم السيبراني يتداخلان أكثر فأكثر. وبفضل قيام الاتحاد بالجمع بين مختلف أصحاب المصلحة ضمن شراكة عالمية فإنه يتصدر الصفوف في ميدان توفير الحلول اللازمة، السياساتية منها والتقنية، لمكافحة الأخطار السيبرانية.

تشكل مبادرة حماية الأطفال على الخط (COP) شبكة عمل تعاونية ترمي إلى تحديد المخاطر وأوجه الضعف التي يتعرض لها الأطفال في الفضاء السيبراني على مستوى العالم، وإرساء الوعي، واقتسام الموارد، واستحداث أدوات عملية للمساعدة على التقليل من الأخطار وترويج المواطنة الرقمية المسؤولة.

وكان من بين التطورات الرئيسية في هذا الصدد وضع البرنامج العالمي للأمن السيبراني (GCA) الذي يشكل إطاراً دولياً للتعاون. وييسر هذا البرنامج جهود الاتحاد لبناء القدرة التقنية الضرورية لمساعدة البلدان على مجابهة التهديدات السيبرانية، والتوصية بمعايير دولية بشأن الأمن والتكنولوجيا السيبرانيين، والعمل كمحفل للمناقشات حول المعارف والسياسات العامة.

التصدي للهجمات السيبرانية الوطنية

يمكن أن تعيث هجمة سيبرانية وطنية فساداً بالبنية التحتية الحاسمة، وأن تخلّف أثراً مباشراً على مظاهر الحياة اليومية وهو ما يمتد من تعذر الوصول إلى الحسابات المصرفية إلى انقطاع شبكات النقل، واختلال إمدادات الطاقة الكهربائية، ومنع الاتصالات، وظواهر أسوأ من ذلك.

وثمة حاجة جلية إلى بنى مؤسسية فعّالة للتصدي للحوادث والهجمات السيبرانية. ويعمل الاتحاد مع الدول الأعضاء، والأقاليم، وشركاء الصناعة، لنشر الإمكانيات اللازمة لبناء القدرات على المستويين الوطني والإقليمي.

ويسعى الاتحاد إلى بناء القدرات والخبرات عبر برامج واسعة للتدريب والدعم. وتشمل مثل هذه المبادرات ما يلي:

- مساعدة 50 دولة عضواً على تقييم قدراتها الوطنية المتعلقة بالتأهب والتصدي في مجال الأمن السيبراني. وتلقت سبع دول أعضاء العون لإنشاء فريق وطني للتصدي للحوادث الحاسوبية (CIRT)، إلى جانب سبع دول أخرى ستتلقى مساعدة الاتحاد في هذا الميدان بصورة مؤكدة.

- تم حتى اليوم إجراء سبعة تدريبات سيبرانية للفرق الوطنية للتصدي للحوادث الحاسوبية ضمت أكثر من 60 بلداً. وهي تشمل تقييم الوظائف الأساسية للفرق الوطنية التي أنشئت لتحديد ما إذا كانت متوافقة مع المعايير الدولية وأفضل الممارسات.

- يتسم رسم استراتيجيات وطنية للأمن السيبراني بصعوبة بالغة بالنسبة لأقل البلدان نمواً (LDC) نظراً إلى افتقارها إلى الأطر القانونية والتنظيمية الكافية، وقلة الخبرات/الموارد البشرية والمالية اللازمة لتحديد التهديدات السيبرانية وإدارتها والتصدي لها. ويساند مشروع الاتحاد المعنون "تعزيز الأمن السيبراني في أقل البلدان نمواً" هذه البلدان على تعزيز قدراتها المتعلقة بالأمن السيبراني لضمان تعزيز حماية بنيتها التحتية الوطنية واستخلاص الفوائد الاجتماعية والاقتصادية القصوى.

- وعلى المستوى الإقليمي يجري تقديم المزيد من المساعدة في صيغة المراكز الإقليمية للأمن السيبراني التابعة للاتحاد، وهي مراكز فعلية تستضيفها الدول الأعضاء ومن ثم تعمل كنقاط

اطلعوا على مزيد من المعلومات عن أنشطة الاتحاد الدولي للاتصالات في مدونة الاتحاد الإلكترونية:
http://itu4u.wordpress.com

اتصال إقليمية للاتحاد فيما يتصل بمسائل الأمن السيبراني. ويتخذ المركز الإقليمي العربي للأمن السيبراني من عُمان مقراً له، وثمة خطط قيد التنفيذ حالياً لإنشاء المركز الإقليمي الإفريقي للأمن السيبراني في نيجيريا.

يعتبر الأمن عنصراً أساسياً في توصيات الاتحاد ومعاييره، وتستعرض كل لجان الدراسات التابعة له حالياً وبصورة اعتيادية المسائل المرتبطة بالأمن كجزء من عملها.

- يساعد الاتحاد الدول الأعضاء على تفهم الجوانب القانونية للأمن السيبراني لتمكينها من مواءمة أطرها الدولية لتغدو قابلة للتطبيق والتشغيل على المستوى الدولي.

- يعني الدور المتصاعد لتكنولوجيا المعلومات والاتصالات في ميادين الخدمات المتنوعة مثل الصحة، والتعليم، والمجالات المالية والتجارية، أن هناك حاجة متزايدة لبيئة سيبرانية آمنة تماماً، ومع ذلك فإن هناك افتقاراً عالمياً مزمناً إلى المهنيين المؤهلين في الأمن السيبراني. وللمساعدة على سد هذه الثغرة فقد نظم الاتحاد حلقات عمل تدريبية للأمن السيبراني شارك فيها أكثر من 1 900 من المسؤولين الحكوميين، والعاملين في الهيئات التنظيمية، ومهنيي تكنولوجيا المعلومات والاتصالات من القطاعين العام والخاص من مختلف أنحاء العالم.

حماية الأطفال على الخط (COP)

يندرج الأطفال في عداد أكثر المجموعات ضعفاً على الخط حيث يمثلون الجيل الجديد من 'المواطنين الرقميين' ويكونون على استعدادٍ عالٍ للغاية للكشف عن بياناته الشخصية على الخط مما يجعله هدفاً سهلاً للمجرمين والقراصنة.

وتتلاشى يوماً بعد يوم الفواصل القائمة بين العالمين السيبراني والواقعي، مما يخلّف عواقب خطيرة على عافية الأطفال العقلية والبدنية. وخلال مسح أخير أفادت نسبة تقرب من نصف المراهقين الذين تتراوح أعمارهم بين الثالثة عشرة والسابعة عشرة أنهم عانوا من شكل ما من أشكال الترهيب السيبراني في العام الماضي. ومما يثير القلق بشكل أكبر أن ثلاثة أرباع الشباب الذين طالتهم الإغراءات الجنسية العدوانية في العالم الحقيقي قد التقوا بالمعتدين عليهم على الخط.

وتشكل مبادرة حماية الأطفال على الخط (COP) شبكة عمل تعاونية ترمي إلى تحديد المخاطر وأوجه الضعف التي يتعرض لها الأطفال في الفضاء السيبراني على مستوى العالم، وإرساء الوعي، واقتسام الموارد، واستحداث أدوات عملية للمساعدة على التقليل من الأخطار وترويج المواطنة الرقمية المسؤولة. وفي إطار هذه المبادرة يعمل أكثر من 54 شريكاً دولياً من الحكومات، والقطاع الخاص، والمجتمع المدني، والهيئات الأكاديمية، والمنظمات الدولية جنباً إلى جنب لتحقيق هذه الأهداف.

المعايير التقنية (توصيات)

تضطلع المعايير التقنية للاتحاد (المعروفة باسم التوصيات) بدور رئيسي في حماية المستخدمين على الخط. وتحتل لجنة الدراسات 17 لقطاع تقييس الاتصالات موقع الصدارة بين لجان الدراسات فيما يتعلق بأمن الاتصالات وإدارة الهوية، مع تركيز أساسي على بناء الثقة والأمن في ميدان استخدام تكنولوجيا المعلومات والاتصالات.

ويعتبر الأمن عنصراً أساسياً في توصيات الاتحاد ومعاييره، وتستعرض كل لجان الدراسات التابعة له حالياً وبصورة اعتيادية المسائل المرتبطة بالأمن كجزء من عملها. وتشمل الإنجازات المحققة حتى هذا التاريخ ما يلي: التوصيات التقنية لشبكات بروتوكول الإنترنت (IP)، ومعايير شبكات الجيل التالي (NGN)، وضمان مبادئ أمن واضحة للشبكات الخلوية المتنقلة في عالم اليوم والغد. ومن الأمثلة البارزة على ذلك التوصية **X.509** الصادرة عن قطاع تقييس الاتصالات بشأن البنية التحتية الوطنية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI). وتحدد التوصية المذكورة، ضمن جملة أمور، النماذج المعيارية لشهادات المفاتيح العمومية، وقوائم إبطال الشهادات، وشهادات النعوت.

النهج العالمي لأصحاب المصلحة المتعددين

- نتيجة الاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات في أقل البلدان نمواً (LDC) فإن الأمن السيبراني يكتسب أولوية متصاعدة، علماً بأن الدراسات تشير إلى أن البلدان النامية هي الأكثر هشاشة إزاء الجرائم السيبرانية والتهديدات السيبرانية. ويركز مشروع الاتحاد المعنون "تعزيز الأمن السيبراني في أقل البلدان نمواً" على حماية المستخدمين وتدعيم أمن الإنترنت من خلال توفير المساعدة على مستوى السياسات.

- أبرم الاتحاد اتفاق شراكة مع شركة ABI Research بشأن مؤشر الأمن السيبراني العالمي (GCI) لتوفير علامات قياس للقدرات الوطنية للأمن السيبراني وتمكين الدول الأعضاء من التعلم من أفضل الممارسات.

- أرسى الاتحاد أيضاً تعاوناً رسمياً مع شركات الأمن السيبراني مثل Symantec و Trend Micro لتبادل المعلومات بصورة منتظمة عن الاتجاهات الحالية والناشئة للتهديدات السيبرانية.

- يعمل الاتحاد حالياً مع الوكالات/الهيئات الأخرى في منظومة الأمم المتحدة لتعزيز التنسيق الداخلي بين وكالات الأمم المتحدة في مساعدتها للدول الأعضاء فيما يتصل بالأمن السيبراني.