مركز البيان للدراسات والتخطيط
Al-Bayan Center for Planning and Studies

التكاليف الخفية للجرائم السيبرانية

زانا مالكوس سميث ويوجينيا لوستري
مدير المشروع: جيمس أ.لويس

سلسلة إصدارات مركز البيان للدراسات والتخطيط

عن المركز

مركزُ البيان للدراسات والتخطيط مركز مستقلٌّ، غيرُ ربحيّ، مقرّه الرئيس في بغداد، مهمته الرئيسة -فضلاً عن قضايا أخرى- تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاصٍ ومنطقة الشرق الأوسط بنحو عام. ويسعى المركز إلى إجراء تحليل مستقلّ، وإيجاد حلول عمليّة جليّةٍ لقضايا معقدة تهمّ الحقليْن السياسي والأكاديمي.

ملاحظة:

الآراء الواردة في المقال لا تعبر بالضرورة عن اتجاهات يتبناها المركز، وانما تعبر عن رأي كتابُها.

www.bayancenter.org

info@bayancenter.org

Since 2014

التكاليف الخفية للجرائم السيبرانية

زانا مالكوس سميث ويوجينيا لوستري - مدير المشروع: جيمس أ.لويس *

ترجمة ومراجعة: د. باسم علي خريسان

أولاً: التكاليف الخفية للجرائم السيبرانية: التكلفة العالمية.

يبدو أن الجرائم السيبرانية لا يمكن وقفها، فهنالك الآلاف من الجرائم السيبرانية تحدث كل عام، وتتراوح تكلفتها من بضع مئات من الدولارات إلى الملايين، إذ تستمر مخاطر الجرائم السيبرانية في النمو على عمليات وأرباح العديد من المؤسسات، ويمكن أن يكون الوقت المستغرق في معالجة حادث سيبراني طويلاً؛ لذلك يتعين على الشركات والوكالات بذل المزيد من الجهد لمنع وقوع الحوادث السيبرانية، ويحتاجون أيضاً إلى بذل المزيد من الجهد لتسريع استعادة الخدمة، ومعالجة اضطرابات الأعمال، وإصلاح الأضرار التي تلحق بمعنويات الموظفين وثقة العملاء.

باستخدام الانموذج الذي تم تطويره لتقارير سابقة، نقدر التكلفة النقدية للجرائم السيبرانية بحوالي (945)مليار دولار، أو ما يزيد قليلاً عن (1%) من الناتج المحلي الإجمالي العالمي، هذه الزيادة تعد كبيرة عن تقديراتنا للعام 2018 بحوالي (600) مليار دولار، أفضل التقارير تفسر بعض الزيادة، ومع ذلك، من الواضح أن الجريمة السيبرانية تستمر في النمو بسرعة، مع توقع ان يتجاوز الإنفاق العالمي على الأمن السيبراني (145) مليار دولار في عام 2020، لتشكل الجرائم السيبرانية عبئاً قيمته (1) تريليون دولار على الاقتصاد العالمي.

تتزايد الجرائم السيبرانية لأنها مربحة، ويمكن أن تكون سهلة، ويمكن أن تكون المخاطر التي يتعرض لها مجرمو الإنترنت منخفضة، على الرغم من أن تطبيق القانون السيبراني قد تحسن أيضاً، إلا أن أكثر المجرمين السيبرانيين قدرة يفلتون عادة من المحاكمة والعقاب، تتزايد الجرائم السيبرانية أيضاً لاعتمادنا على الفضاء السيبراني في إدارة حياتنا اليومية وأعمالنا، فالتبني الأسرع للتقنيات

* مركز الدراسات الاستراتيجية والدولية 2020.

الجديدة مثل الذكاء الاصطناعي (AI)[1] وتقنية تزيين الصور والفيديوهات العميقة، بواسطة مجرمي الإنترنت، يمنحهم ميزة ويفسر بعضاً من هذه الزيادة، خلاصة القول إن الجرائم السيبرانية آمنة ومربحة، وتحدث في بيئة تتوسع باستمرار وتزدهر في الأنظمة الضعيفة.

إن أبرز أشكال الجرائم السيبرانية هي التجسس الاقتصادي وسرقة الملكية الفكرية والجرائم المالية، وبشكل متزايد (برامج الفدية)[2]، فهي مسؤولة عن أكبر الخسائر، ونقدر أن سرقة الملكية الفكرية والجرائم المالية يمثلان ثلثي الخسائر المالية ويشكلان أكبر تهديد للشركات، ويقترن ذلك بمجموعة من الجرائم ضد المستهلكين والشركات الصغيرة، التي عادة لا تنطوي على خسائر كبيرة ولكن يمكن أن تؤثر على الآلاف من الأفراد.

مع ذلك، فإن التكاليف الخفية الأخرى التي تدفعها الشركات والمستهلكين، فضلاً عن الخسائر المباشرة، هي محور هذا التقرير، إذ تعد سرقة معلومات الهوية الشخصية (PII)[3] والأصول النقدية أمراً دراماتياً وضاراً، ولكن قد تأتي التكلفة الأكثر أهمية للجريمة السيبرانية من الضرر الذي يلحق بأداء الشركة والأضرار الإجمالية التي تلحق بالاقتصادات الوطنية.

1-الاذكاء الاصطناعي: (Artificial Intelligence)، وهو سلوك وخصائص معينة تتسم بها البرامج الحاسوبية، تجعلها تحاكي القدرات الذهنية البشرية وأنماط عملها. من أهم هذه الخاصيات القدرة على التعلم والاستنتاج ورد الفعل على أوضاع لم تبرمج في الآلة. إلاّ أنَّ هذا المصطلح جدلي نظراً لعدم توفر تعريف محدد للذكاء الاصطناعي الذي هو فرع من علم الحاسوب. تُعرِّف الكثير من المؤلفات الذكاء الاصطناعي، على أنه: «دراسة وتصميم العملاء الأذكياء»، والعميل الذكي هو نظام يستوعب بيئته ويتخذ المواقف التي تزيد من فرصته في النجاح في تحقيق مهمته أو مهمة فريقه. https://ar. wikipedia. org/wiki/

2- برامج الفدية (المعروف أيضاً باسم مبرمج الملفات) :هي نوع من البرمجيات الخبيثة تقوم بتأمين جهازك أو تشفير المحتوى الموجود على الجهاز وتقوم بابتزاز المال منك لاستعادة الوصول إلى المحتوى الخاص بك. قد يحتوي هذا النوع من البرامج الضارة أيضاً على موقت مدمج مع موعد نهائي للدفع مبرمج مسبقاً ويجب الوفا به. وفي حال عدم الوفاء بالموعد النهائي، يرتفع السعر أو يصبح الجهاز غير قابل للوصول بشكل أساسي. عندما يكون الجهاز مصاباً، قد يحاول مبرمج الملفات تشفير محركات الأقراص المشتركة الموجودة على الجهاز. تبدو هذه العملية كما لو أن البرمجيات الخبيثة تنتشر عبر الشبكة، لكنها ليست كذلك في الواقع. يحدث هذا الموقف عند تشفير محرك الأقراص المشترك على خادم ملف، لكن الخادم ذاته لا يحتوي على برامج ضارة (ما لم يكن خادماً طرفياً). https://help. eset. com/glossary/ar-EG/ransomware. html

3-معلومات الهوية الشخصية (PII) :هي أي بيانات يمكن استخدامها لتحديد هوية فرد معين، تم اعتبار أرقام الضمان الاجتماعي، وعنوان البريد أو البريد الإلكتروني، وأرقام الهواتف بشكل شائع معلومات تحديد الهوية الشخصية، ولكن التكنولوجيا وسعت نطاق معلومات تحديد الهوية الشخصية بشكل كبير، يمكن أن يتضمن عنوان (IP) أو معرفات تسجيل الدخول أو منشورات الوسائط الاجتماعية أو الصور الرقمية. ويمكن أيضاً تصنيف بيانات تحديد الموقع الجغرافي والقياسات الحيوية والسلوكية على أنها معلومات تحديد الهوية الشخصية.

https://www. csoonline. com/article/3215864/how-to-protect-personally-identifiable-information-pii-under-gdpr. html

تشمل مصادرنا في اعداد هذا التقرير على نتائج استطلاع الرأي الذي شمل (1500) مدير تنفيذي من جميع أنحاء العالموبيانات منشورةومقابلات وتقديرات من الوكالات الحكومية والشركات في البلدان الأخرى.

لقد تعرض ثلثا الشركات التي شملها الاستطلاع لنوع من الحوادث السيبرانية في العام 2019، وكان متوسط توقف العمل 18 ساعة وكان متوسط التكلفة لأغلى حادثة أكثر من نصف مليون دولار، وذكرت جميع الشركات المتضررة تقريباً أن التكاليف تجاوزت الخسارة المالية، وتمثلت أكبر الخسائر غير المالية في الإنتاجية وساعات العمل الضائعة، وبشكل مثير للدهشة، قالت أكثر من نصف المؤسسات التي شملتها الدراسة إنه ليس لديهم خطة لمنع وقوع الحوادث السيبرانية والاستجابة لها.

من جهة أخرى وجدنا نقصاً في الفهم على مستوى المؤسسة للمخاطر السيبرانية؛ مما يجعل الشركات والوكالات عرضة لأساليب الهندسة الاجتماعية المتطورة، وبمجرد اختراق المستخدم، لن تتمكن المؤسسات من التعرف على المشكلة في الوقت المناسب لمنع انتشار البرامج الضارة، فضلاً عن ذلكادى الاستخدام المتزايد – والذي لا مفر منه – للأجهزة الشخصية مثل الهواتف الذكية أو الأجهزة اللوحية إلى توسيع سطح الهجوم والنقاط النهاية للهجوم وتعقيد إدارة الدفاع السيبراني.

التكاليف غير النقدية

للجرائم السيبرانية العديد من التكاليف الخفية –من تكاليف الفرصة والوقت والمال الذي يتم إنفاقه على اتخاذ قرارات الأمن السيبرانيوتأثير التوقفوفقدان الإنتاجية والضرر الذي يلحق بالعلامة التجارية والصورة– معظم هذه التكاليف ليس لها قيمة بالدولار ويمكن تحديدها بسهولة، مع ذلك يجب علينا أخذها في الحسبان عند تقييم تأثير الجريمة السيبرانية.

تكاليف الفرصة

تكلفة الفرصة البديلة هي الدخل (أو الإنتاج) المفقود عندما يتعذر استخدام الموارد أو عدم تقديم خدمة بسبب حادث سيبراني، وجدنا أن تكاليف الفرصة البديلة، مثل فقدان المبيعاتوانخفاض الكفاءةوالاضطراب الكلي للأعمال المعتادة، تشكل نسبة كبيرة من الآثار غير المباشرة.

يحتاج حساب تكلفة الجرائم السيبرانية إلى النظر في تكاليف الفرصة البديلة، مثل الفرص الضائعة أو الفوائد الضائعة التي كان من الممكن الحصول عليها لولا تلك الأنشطة الضارة في

الفضاء السيبراني، ومن الأمثلة على ذلك الإنفاق الإضافي على الأمن السيبراني الذي لن يكون مطلوباً في بيئة أمنة، فضلاًعنضياع المبيعات أو انخفاض الإنتاجية أو اتخاذ قرار بتجنب أو تقييد استخدام الإنترنت لبعض الأنشطة بسبب المخاطر.

لقد حددنا أربعة أنواع من تكاليف الفرصة: انخفاض الإنتاجية وانخفاض الإنفاق على البحث والتطويروالسلوك الذي يتجنب المخاطروزيادة الإنفاق على الدفاعات السيبرانية، من بين (1332) مشاركاً في الاستطلاع تعرضوا لمثل هذه الحودث في العام 2019، استثمر (45%) منهم في برامج الأمان الجديدة، رفعت (39%) من المؤسسات المذكورة الميزانية المخصصة للحوادث الأمنية، وقام (30%) منها بتعيين موظفين جدد لأمن تكنولوجيا المعلومات.

تدفع الشركات علاوات المخاطر بسبب زيادة الجرائم السيبرانية، ويمكن تقدير تكلفة علاوات المخاطر هذه من خلال النظر في معدل النمو في سوق الأمن السيبراني، في العام 2019، بلغت قيمة سوق الأمن السيبراني العالمي حوالي (145) مليار دولار، في حين كانت(113) مليار دولار في العام 2015، ولا تحتاج المؤسسات النظر في الخسائر المباشرة فحسب، بل تحتاج أيضاً إلى النظر للتكاليف الناتجة عن تعطل الأعمال ووقت التوقف عن العملوالفرص الضائعة.

ويمكن أن تؤدي الجرائم السيبرانية كذلك إلى سلوك يكره من قبل كل من المؤسسات والأفراد، أن تكون ضحية للجرائم السيبرانية هي تجربة مؤلمة، نظراً للمخاوف بشأن الكشف عن المعلومات الشخصية أو التأثير المالي، بصرف النظر عن ترك الضحايا منزعجين أو غاضبين أو حتى خجولين، فقد تؤدي الجرائم السيبرانية أيضاً إلى انخفاض المشاركة عبر الإنترنت، أصبح الانتقال عبر الإنترنت أمراً لا مفر منه بشكل متزايد، ولاسيما أثناء عمليات إغلاق بسبب (COVID-19)، أظهرت بيانات الاستطلاع أن مخاوف الخصوصية والأمان منعت بعض الأسر من الانخراط في أي نشاط عبر الإنترنت، في حين أن الإحجام عن المشاركة عبر الإنترنت قد انخفض، حيث كانت هنالك زيادة مقابلة في القلق العام بشأن الخصوصية في العديد من البلدان، ولا تنبع مخاطر الخصوصية دائماً بشكل مباشر من الجرائم السيبرانية، ولكنمن الانتهاكات البارزةالتي تخلق إحساساً واسع النطاق بالمخاطر عندما يتعلق الأمر بالحضور على الإنترنت.

في الوقت الحاضر، هنالك إعادة تقييم واسعة النطاق لتكاليف الخصوصية التي يمكن للنشاط عبر الإنترنت أن يخلقها، ويزيد من الوعي بضرورة حماية المؤسسات لبيانات مستخدميها، مصحوبة

بطلب متزايد للتنظيم، وتجدر الإشارة إلى أنه على الرغم من المزاعم المعتادة من المؤسسات بأنها عانت من هجمات "معقدة للغاية" كان من المستحيل استباقها، فإن معظمها يعاني من بعض نقاط الضعف الأكثر شيوعاً ويفشل في اتباع أفضل الممارسات المعروفة.

وقت تعطل النظام

وقت التوقف عن العمل هو النتيجة الطبيعية لحادث أمن تكنولوجيا المعلومات –الوقت الذي لا يمكن خلاله استخدام التكنولوجيا والأنظمة في المستوى الطبيعي للوظائف، سواء كانت برامج الفدية تمنع الوصول إلى أنظمة وبيانات المؤسسة أو تحتاج إلى إعادة تعيين لمواجهة أي تدخل–فإن إزالة الوصول إلى الانظمة التكنولوجية يؤثر بشكل كبير على المؤسسات ويمكن أن يمنع التطوير المنتظم للعمليات، ما يؤثر على كل من الموظفين والمستهلكين معا، وجدنا أن فترة التوقف عن العمل هي تجربة شائعة لحوالي ثلثي المؤسسات التي شملها الاستطلاع.

بلغ متوسط الأثر المالي للتوقف عن العمل لأي قسم في المؤسسة ما يقارب (590) ألف دولار، بالنسبة لـ (33%) من الذين شملهم الاستطلاع، تراوحت التكلفة بين (100000 و 500000) دولار، ليس من المستغرب أن تتعرض الأقسام الهندسية لخسائر أكبر بمتوسط (965) ألف دولار، في تناقض حاد مع إدارات الموارد البشرية، التي تكبدت خسائر بنحو (89) ألف دولار، قد تواجه الأقسام الهندسية تكاليف أعلى بسبب متطلباتها للوصول إلى ملفات وبرامج معينة تعد جزءاً لا يتجزأ من العمليات اليومية للشركة، كانت تكلفة الاختراق فيها، في المتوسط، أكثر 10 مرات من تكلفة الموارد البشرية (HR).

أظهر الاستطلاع الذي أجريناه أنه من بين (1500) مشارك، أفاد (68%) أنهم عانوا من تعطل بسبب حوادث أمن تكنولوجيا المعلومات، وعادة ما تستمر أقل من يوم. في المتوسط، استمرت أطول فترة توقف بسبب حادث أمن تكنولوجيا المعلومات 18 ساعة، يعد التوقف عن العمل لأكثر من يومين أمراً غير معتاد، حيث عانى أقل من (1%) من فترات التوقف عن العمل لأكثر من سبعة أيام.

حادثة أمن تكنولوجيا المعلومات الأخيرة التي تعرضت لها شركة ((Avon[4]، على سبيل المثال، جعلت الوصول إلى أنظمة الشركة غير قابل للاستخدام لمدة شهر تقريباً، تم الكشف عنه إلى لجنة الأوراق المالية والبورصات الأمريكية في 9 حزيران (لم يتم تأكيد طبيعته في وقت كتابة هذا التقرير) أثر على العمليات في المملكة المتحدة البريطانية والأرجنتين والبرازيل وبولندا ورومانيا، ما جعل أنظمة (Avon) الخلفية تمنع المستخدمين من تقديم الطلبات، وتجبر الموقع على عدم الاتصال بالإنترنت، وتقلص المبيعات عبر الإنترنت، وتمنع وصول عمالها إلى الأنظمة والمستندات.

وقد أفاد أحدث تقرير للجنة الأوراق المالية والبورصات في 26 تموز أن (Avon) قد ''أعادت تأسيس معظم أنظمة التشغيل الخاصة بها واستأنفت عملياتها في معظم أسواقها''، سيكون من الصعب تحديد الاثر المالي لهذا الحدث، خاصة وأنه حدث ذلك في خضم جائحة(COVID-19)، إذ يذكر -على سبيل المثال- أن تقرير (Avon) الفصلي الصادر في أيار أوضح أنه في ذلك الوقت لم يتمكنوا من تقدير التأثير طويل المدى للشلل الاقتصادي الناجم عن الجهود المبذولة؛ للحد من انتشار فيروس ((COVID-19 والانخفاض المتوقع في نشاط أعمال ونتائج العمليات والوضع المالي للشركة.

ولكن حتى إذا لم يتجاوز وقت التعطل لكل حادث يوماً واحداً، فالحوادث المتكررة التي تتسبب في حدوث توقف يصل إلى فترات كبيرة لا تتمكن فيها المؤسسات من استخدام أنظمتها كما هو متوقع، فقد كشفت طلبات حرية المعلومات المرسلة إلى الجامعات البريطانية أنها تعاني من توقف لمدة أسبوع تقريباً كل عام، في المتوسط، ''عانوا من 18 انقطاعاً غير مخطط له سنوياً، في آذار 2019، أصاب هجوم ببرنامج الفدية شركة نورسك هايدرو(Hydro Norsk)[5]، وهي

4-(Avon) شركة أفون للمنتجات: هي شركة تسويق متعددة المستويات في الجمال والأسرة والعناية الشخصية. بلغت مبيعات أفون السنوية (5، 5) مليار دولار في جميع أنحاء العالم في العام 2018. وإنها خامس أكبر شركة تجميل، وهي ثاني أكبر مؤسسة للبيع المباشر في العالم (بعد أمواي). الرئيس التنفيذي للشركة هو جان زيديرفيلد، الذي تم تعيينه في هذا المنصب في شباط 2018. في ايار2019، أعلنت شركة ناتورا & كو البرازيلية عن عزمها على شراء أفون. https://ar. wikipedia. org/wiki/

5- نورسك هايدرو Norsk Hydro (يشار إليها غالباً باسم هايدرو) :هي شركة نرويجية للألمنيوم و الطاقة المتجددة، ويقع مقرها الرئيس في أوسلو. وهي واحدة من أكبر شركات الألمنيوم في جميع أنحاء العالم، لديها عمليات في حوالي 50 دولة حول العالم وتنشط في جميع القارات، تمتلك الدولة النرويجية (34، 3%) من الشركة من خلال وزارة التجارة والصناعة والثروة السمكية، وتمتلك فولكيتريغدفوند نسبة (6. 5%) أخرى، والتي يديرها الصندوق التقاعدي الحكومي النرويجي، توظف نورسك هيدرو ما يقرب من (35000) شخص، تشغل هيلدي ميريت آشيم منصب الرئيس التنفيذي منذ ايار 2019. كان لشركة نورسك هايدرو حضور كبير في صناعة النفط والغاز حتى تشرين الاول 2007، عندما تم دمج هذه العمليات مع ستات أويل لتشكيل ستات أويل هايدرو (في عام 2009 تغيرت مرة أخرى إلى ستات أويل، والتي تسمى الآن إكوينور). https://ar. wikipedia. org/wiki.

شركة نرويجية لتصنيع الألمنيوم تعمل في (40) دولة، تقدر التقارير الإعلامية أن هجوم برامج الفدية قد كلف الشركة حوالي (71) مليون دولار، مما أثر على الشركة بأكملها، وأثر على العمليات في العديد من البلدان وتسببفي محدودية القدرة الإنتاجية لفترة طويلة من الوقت، على سبيل المثال، رفعت مصفاة (Alunorte)[6] في البرازيل القيود المفروضة على مصنعها بحلول شهر أيار فقط، حيث كانت تعمل بنسبة (80%) من طاقتها بحلول شهر حزيران وأعلنت (Hydro Norsk) أنها استأنفت عملياتها العادية بحلول تشرين الثاني 2019 فقط.

انخفاض الكفاءة

خسرت المؤسسات، في المتوسط ، تسع ساعات عمل عند تعرضها لوقت تعطل، على سبيل المثال، أدى هجوم (ransomware NotPetya)[7] إلى إغلاق موقتلشركة الشحن الدنماركية (Maersk)[8] المسؤولة عنما يقرب من (20%) من احتياجات الشحن في العالم، كانت الخسارة في حدود ثلاثة مليارات دولار ".

تأثرت شركة دولية كبرى أخرى، وهي شركة التوصيل العالمية(FedEx)، التي خسرت ما يقرب من" (300) مليون دولار بعد تعطل عمليات وحدة(TNTExpress) التابعة للشركة في أوروبا، بالإضافة إلى شركة الأدوية الأمريكية (Merck) وشركة النفط الروسية[9] (Rosneft).

6- Hydro Alunorte: هي أكبر مصفاة للألومينا في العالم خارج الصين وتقع في مدينة باركارينا بولاية بارا.
https://www. hydro. com/en/about-hydro/hydro-worldwide/north-america/ . /azil/barcarena/alunorte

7- بداء هجوم (Petya ransomware) بالانتشار دولياً في 27 حزيران 2017. استهداف الخوادم Windows وأجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة، بدا أن هذا الهجوم هو نسخة محدثة من فيروس Petya الضارة. استخدم ثغرة Server Message Block التي استخدمها WannaCry للانتشار إلى الأجهزة غير المصححة، بالإضافة إلى تقنية سرقة بيانات الاعتماد، للانتشار إلى الأجهزة غير المعرضة للخطر. كان بيتيا هجوماً سيبرانياً عالمياً تم الشعور به في جميع أنحاء العالم، لكنه استهدف أوكرانيا بشكل أساسي خلال تشغيله في حزيران 2017.

https://www. mcafee. com/enterprise/en-us/security-awareness/ransomware/petya. html

8- ميرسك سيلان (Mærsk) : وهي شركة دنماركية للنقل البحري تاسست في كوبنهاغن في العام 1904م وتعد من أكبر الشركات العاملة في مجال الحاويات والشحن على مستوى العالم وهي واحدة من عدة شركات ضمن مجموعة شركات ايه بي مولار ميرسك التي تحتوي على مجالات عدة منها ما يرتبط بمجال الحاويات أو المجالات المختلفة الأخرى. تمتلك شركة ميرسك سيلاند أكبر ناقلة بحرية:https://ar. wikipedia. org/wiki/

9- روس نفط (Rosneft) : هي شركة نفط متكاملة أغلبيتها مملوكة للحكومة الروسية، مقرها الرئيس في مقاطعة بلاتشوج، موسكو، بالقرب من الكرملين، على نهر موسكفا. أصبحت روس نفط من الشركات الروسية الرائدة في مجال استخراج وتكرير النفط بعد شراءها أصول عملاق النفط السابق بوكوس في مناقصة حكومية. في اذار 2013، بعد اكتمال إستحوذها على تيإن

إن الكشف عن التكلفة الدقيقة لتعطل الصناعة مثل عدم التسليم وإعادة تركيب المعدات الأساسية هو جزء من القصة، رسم رئيس (Maersk-Møller) صورة قاتمة عند وصفه، لنطاق هائل من الاضطراب الناجم عن هجوم برامج الفدية وصعوبة تحديد مقدار الضرر الناجم: ''تخيل شركة تدخل فيها سفن تحمل من (10 إلى 20) ألف حاوية إلى ميناء كل 15 دقيقة، ولمدة 10 أيام، ليس لديك أي تكنولوجيا معلومات. . . هذا أمر يكاد يكون من المستحيل تخيله''.

قبل هجوم (NotPetya)، وصف موقف شركة (Maersk) للأمن السيبراني بأنه متوسط'' مثل العديد من الشركات، لذلك تسعى الشركة الان إلى ''الحصول على الأمن السيبراني كميزة تنافسية''، كذلك يعد تلف العلامة التجارية وفقدان الثقةوالسمعة نتيجة طويلة الأجل لحوادث أمن تكنولوجيا المعلومات، هذا شيء يجب أن تهتم الشركات بمنعه، اشار (26%) من الذين شملهم الاستطلاع الضرر الذي لحق بالعلامة التجارية من التعطل الذي حدث بسبب الهجوم السيبراني، تعد تكلفة إعادة تأهيل العلامة التجارية أو العمل مع العلاقات الإعلامية أو تعيين موظفين جدد جزءاً من تكلفة الجرائم السيبرانية.

فالسمعة هي في جزء كبير منهامسألة إدراك تصور للإهمال ونقص حماية خصوصية البيانات التي يمكن أن تدفع العملاء بعيداً عن الأعمال التجارية، وجدت دراسة أجريتفي العام 2017 أن (87%) من المستهلكين أشاروا إلى أنهم سيغيرون الموردين إذا لم يثقوا في كيفية تعامل الشركة مع بياناتهم، هذه ليست مسألة منع وقوع حادث حصري، كيف تستجيب المؤسسة وكيف يمكن أن تكون منفتحة وصريحة بشأن الموقف الذي تعيش فيه، يمكن أن تقطع شوطاً طويلاً في الحفاظ على ثقة المستهلكإساءة استخدام بياناتهم، والتوقعات بشأن حمايةالبيانات آخذة في الازدياد.

في الواقع فإن الشفافية وإبلاغ العملاء عندما تكون بياناتهم المالية أو الشخصية قد تم اختراقها ضرورية للحفاظ على الثقة وإدارة الأزمة. فقط (26%) من المؤسسات التي تعرضت لحوادث أمنية في عام 2019 شاركت معلومات حول أكثر الحوادث خطورة مع العملاء.

كيه-بي‌بي، أصبحت روس نفط أكبر شركة نفط :https://ar. wikipedia. org/wiki/

سرقة بروتوكول الإنترنت(**IP**)[10]:

سرقة(IP) جزء من تكلفة الفرصة البديلة للشركات، يمكن تحقيق سرقة (IP) من خلال عدة وسائل، مكتب التحقيقات الفدرالي الامريكي، على سبيل المثال، يحدد التجسس الاقتصادي والجهود السرية والنفوذ الأجنبي الخبيثواستهداف الشركات والجامعات في الولايات المتحدة الامريكية، كتقنيات أنموذجية، لا يجب أن يساوي الحادث الناجح دائماً الخسارة المباشرة إذا لم ينجح الجناة في استخدام(IP) مسروق.

مع ذلك، فإن الطرق التي يمكن أن تؤثر بها على الشركة لا تقتصر على تطوير منتجات أو خدمات منافسةفقد يؤدي التأثير على تدفقات الإيرادات إلى تقليل جهود البحث والتطوير، مقترنة بزيادة في تكلفة رأس المال إذا تم النظر الباللملكية الفكرية من قبل المستثمرين على أنها ليست محمية بشكل كافٍ، تلعب الصين دوراً محورياً في مواجهة مخاطر سرقة IP)). قال وزير الخزانة الأمريكي السابق (هنري إم بولسون)، ''السرقة السيبرانية للشركات هي القضية الاقتصادية الأكثر إثارة للجدل والتي يحتمل أن تدمرها وهو ما نواجهه مع الصينيين، أنها تقوض أمننا الاقتصادي، وتعطي مصداقية للشعور بأن الصين لا تلعب بشكل عادل، ويجعل من الصعب إيجاد أرضية مشتركة.

إن السعي إلى سرقة الـ (IP) الأمريكي، ونسخ المنتج أو الخدمة في الصين، واستبدال

10- بروتوكول الإنترنت (Internet Protocol، اختصارًا: IP): هو بروتوكول الاتصال الأساس في حزمة بروتوكولات الإنترنت ويُشكّل الأساس الذي تعتمد عليه عمليّة توجيه الرزم ضمن الشبكة، ويسمح ذلك بالاتصال بين الشبكات المختلفة، وهو جوهر شبكة الإنترنت. يُعرِّف البروتوكول على أنه فضاءً من العناوين، يُستعمل من قبل الطرفيّات والموجّهات، حيث يحتوي كل منها على بطاقة شبكة واحدة على الأقل، تحصل هذه البطاقة على عناوين من فضاء بروتوكول الإنترنت. وتُسمّى عمليّة امتلاك عنوان من فضاء العناوين استضافة العنوان، وتُسمّى بطاقة الشبكة عندها بالمضيف، من الشائع استخدام هذا المصطلح للإشارة إلى الطرفيّة ككل وليس إلى بطاقة شبكة فقط. يمكن للمُضيف أن يمتلك أكثر من عنوان بروتوكول إنترنت في نفس الوقت، ويُوصف حينها بأنّه مُتعدد الاستضافة. يُحدد البروتوكول بنية خاصة للرزم، تتألف من قسمين رئيسيين، هما الترويسة وقسم المعطيات. تكون الترويسة مُقسّمة إلى عدد من الحقول، وتضمّ المعلومات اللازمة لعمل البروتوكول كرقم الإصدار وعنواني مصدر ووجهة الرزمة بالإضافة لمعلومات أخرى، أما قسم المعطيات فيضمّ المعطيات التي يتمّ تغليفها ضمن الرزمة. تاريخيّاً، كان بروتوكول الإنترنت إحدى الخدمات التي تستخدم قنوات لا تتطلب تهيئة اتصال المقدّمة من قبل بروتوكول التحكّم بالنقل الذي قام كل من فينت سيرف وبوب خان بتطويره في عام 1974. لذلك فإن بروتوكول الإنترنت يعتمد على بروتوكول التحكّم بالنقل لضمان وجود اتصال مُسبق بين مختلف الأطراف، ولهذا تُوصف قنوات بروتوكول التحكّم بالنقل بأنّها تتطلّب تهيئة اتصال ونتيجة لهذه العلاقة الوظيفية، غالباً ما يُشار إلى أنموذج الإنترنت بالشكل (TCP/IP). إنّ أول إصدار مُستقل من بروتوكول الإنترنت هو الإصدار الرابع، ويُشار له اختصاراً، وهو البروتوكول الأساسي في شبكة الإنترنت، الإصدار اللاحق هو الإصدار السادس، ويُشار له اختصاراً (IPv6)
https://ar. wikipedia. org/wiki

الشركات الأمريكية في السوق الصينية، وإذا سارت الأمور على ما يرام، كذلك في السوق العالمية فإن هذا الوضع لنيكون مشكلة للولايات المتحدة الامريكية فقط، وجد استطلاعنا أن سرقة الـ(IP) كانت وراء (11%) من الحوادث الأمنية التي تسببت في أطول فترة تعطل، كان هذا متسقاً عبر مناطق مختلفة، يتعلق أحد الأمثلة التي جاءت في الوقت المناسب لأهمية الحماية من سرقة بروتوكول الإنترنتتمثلت بالتجسس الموجه إلى الباحثين الطبيين أثناء جائحة (COVID-19)، مع وجود العديد من الادعاءات الموثوقة بأن قراصنة روس وصينيين استهدفوا أبحاث اللقاحات. وتوضح هذه الهجمات الجانب غير المالي من الجريمة السيبرانية. في حين أن الميزة الاقتصادية لكونك أول شركة تصمم لقاحاً يمكن حسابها، فمن الصعب تحديد سعر للقيمة السياسية لكونك أول دولة تنتج مثل هذا اللقاح.

تكاليف الاستجابة للحوادث يستغرق الأمر في المتوسط (19) ساعة لمعظم المؤسسات للانتقال من اكتشاف حادثة ما إلى علاجها، ويستلزم هذا عادةً استعادة خدمات تكنولوجيا المعلومات إلى السعة الطبيعية، وإزالة التهديد من النظام، واستعادة البيانات المفقودة، ومع ذلك، في بعض الحالات، لن تنظر المؤسسات في معالجة الحادث حتى يتم تحديد مصدره أو يتم تنفيذ بعض التدابير لمنع وقوع الحادث في المستقبل، يتطلب الأمر جهود ثمانية أشخاص، في المتوسط ، لاكتشاف حادث أمن تكنولوجيا المعلومات والاستجابة له، تتضمن التكاليف المخفية الأخرى للشركات التي سُرقت بيانات العميل فيها تقديم نوع من الحماية أو خدمة التعويض للضحايا، مثل تعويض خسائر الاحتيال أو الوصول برعاية الشركة إلى خدمات مراقبة الائتمان والتنبيه بالاحتيال.

على سبيل المثال، بعد تعرضه لخرقَين للبيانات (في 2018 و2020)، أنشأ فندق ماريوت الدولي مراكز اتصال خاصة للاستجابة لمخاوف العملاء، لقد قدموا للعملاء المتأثرين إمكانية الوصول المجاني إلى برامج مراقبة الائتمان وكشف الاحتيال، وقدمت سلسلة الفنادق للعملاء خدمة مجانية لمدة عام واحد لمراقبة مواقع الويب التي يستخدمها مجرمو الإنترنت لتوزيع المعلومات الشخصية للأشخاص بالإضافة إلى تعويض خسائر الاحتيال. بعد خرق بيانات) (Equifax)[11] لعام

11- Equifax Inc: هي وكالة أمريكية متعددة الجنسيات لإعداد تقارير ائتمان المستهلك وهي واحدة من أكبر ثلاثة وكالات لإعداد تقارير ائتمان المستهلك، جنباً إلى جنب مع Experian و TransUnion (المعروفة معاً باسم «الثلاثة الكبار»). تقوم Equifax بجمع وتجميع المعلومات عن أكثر من 800 مليون مستهلك فردي وأكثر من 88 مليون شركة في جميع أنحاء العالم. بالإضافة إلى البيانات والخدمات الائتمانية والديموغرافية للشركات، تبيع Equifax خدمات مراقبة الائتمان ومنع الاحتيال مباشرة إلى المستهلكين:https://en.wikipedia.org/wiki/Equifax

2017، والذي كشف المعلومات الشخصية لـ (147) مليون شخص، قامت ((Equifax بتسوية الدعوى مع لجنة التجارة الفيدرالية (FTC)[12] والمدعين العامين للولاية ومكتب الحماية المالية للمستهلك مقابل دفع (425) مليون دولار ووافقت على تقديم مزايا اضافية حيث أصبح يحق للمستهلكين الأمريكيين تلقي سبعة تقارير ائتمانية مجانية من (Equifax) سنوياً حتى العام 2026.

بينما يمكن إدارة العديد من الهجمات السيبرانية داخلياً، غالباً ما تتطلب الحوادث الكبرى التعاقد مع استشاريين خارجيين بمعدلات عالية، ما يشكل جزءاً كبيراً من تكلفة حادث واسع النطاق، أفادت (213) فقط من بين (1332) مؤسسة شملها الاستطلاع أنها تعاملت مع حوادث الإنترنت دون دعم من طرف ثالث، عادة، كانوا يعتمدون على مؤسسات الأمن السيبراني أو فرق الاستجابة للمساعدة في الاحتواء والتعافي والمعالجة، سواء كان فريق استجابة خارجي أو شركة متخصصة في الأمن السيبراني أو المساعدة القانونية والعلاقات العامة، اعتمدت معظم الشركات على الدعم الخارجي، في معظم هذه الحالات، تم الاستعانة بالاستشاريين للمساعدة في الاحتواء والتعافي والمعالجة، ولكن في(22%) من الحالات، قدموا أيضاً مساعدة في العلاقات العامة، و قدم (14%) منهم المساعدة القانونية.

تأمين مخاطر الإنترنت

أصبح التأمين ضد المخاطر السيبرانية أمراً طبيعياً أيضاً للشركات الكبيرة التي يمكن أن تتوقع بشكل معقول مواجهة هجوماً سيبرانياً في مرحلة ما، ولكن قد يكون من الصعب تبرير الشركات الصغيرة والبلديات التي قد تختار التأمين الذاتي بدلاً من إضافة قسط تأمين كبير.

غالباً ما تكون سياسات التأمين على الإنترنت عبارة عن عقود معقدة للغاية يمكن أن تصل بسهولة إلى مئات الصفحات، ويمكن أن تتوقف المدفوعات عند تعريفات دقيقة لمصطلحات مثل ''نظام الكمبيوتر'' أو ''الحادث السيبراني'' أو على احتياطات الأمن السيبراني المحددة التي

12- لجنة التجارة الفيدرالية (FTC) :هي وكالة مستقلة تابعة لحكومة الولايات المتحدة الامريكية وتتمثل مهمتها الرئيسة في إنفاذ قانون مكافحة الاحتكار المدني (غير الجنائي) الأمريكي وتعزيز حماية المستهلك. تشترك لجنة التجارة الفيدرالية في الاختصاص القضائي على إنفاذ مكافحة الاحتكار المدني الفيدرالي في الولايات المتحدة الامريكية مع قسم مكافحة الاحتكار بوزارة العدل الأمريكية. يقع المقر الرئيس في مبنى لجنة التجارة الفيدرالية في واشنطن العاصمة:

https://en. wikipedia. org/wiki/Federal_Trade_Commission

تم تنفيذها أو لم يتم تنفيذها، لهذه الأسباب، حصلت (28، 4%) فقط من المطالبات في عام 2017 على اموال من شركات التامين، بمتوسط دفع (188، 525) دولاراً أمريكياً، وهو أقل بكثير من متوسط التكلفة البالغ (590) ألف دولار التي وجدناها للهجمات السيبرانية، في هجوم NotPetya))، حاول المتضررين من الاختراق جمع السياسات وأخبرتهم شركات التأمين الخاصة بهم أن الهجمات لن تتم تغطيتها بسبب بنود ''استبعاد الحرب''، هذه النزاعات بين الشركات التي تعرضت لهجمات سيبرانية وشركات التأمين تشق طريقها عبر المحاكم الأمريكية وتسلط الضوء على عدم نضج سوق التأمين السيبراني، الذي يفتقر إلى البيانات الكافية للنماذج (الاكتوارية)[13] الموثوقة، والمخاطر المتطورة باستمرار، والتغطية المتنازع عليها عند مقارنتها بالمخاطر التقليدية مثل الحرائق أو الفيضانات.

ومع ذلك، يستمر السوق في النمو، وتصل قيمته الاجمالية وفق أحد التقديرات إلى مبلغ (5، 5) مليار دولار في عام 2020، ويشمل ذلك سياسات الإنترنت المستقلة، بالإضافة إلى إجراءات الحماية المجمعة في سياسات الملكية والمسؤولية.

الإضرار بمعنويات الموظفين

أفاد العديد من موظفي شركة سوني بتزايد قلقهم بشأن أمنهم الشخصي، حتى أن بعض الموظفين تلقوا رسائل بريد إلكترونية تهددهم بالعنف أو وتهدد عائلاتهم، أدى الكشف عن المعلومات الشخصية، بما في ذلك أرقام الضمان الاجتماعي والمعلومات الطبية، إلى مخاوف بين الموظفين، وفي النهاية، إلى دعوى قضائية جماعية ضد شركة Sony لفشلها في حماية المعلومات، اظهر اختراق شركة Sony العديد من القضايا الداخليةشكلت فضيحة عامة، بما في ذلك بعض القضايا المتعلقة

13- الاكتوارية : علم الاكتواري أو علم حسابات التأمين أو علم إحصائيات التأمين هو علم و مبحث علمي يَستخدم الطرق الحسابية والإحصائية لتقدير حجم المخاطر في قطاع التأمين والصناعات المالية. والاكتواريون هم هؤلاء الأشخاص المؤهلون من حيث التعليم والخبرة في هذا المجال. تضم العلوم الاكتوارية عدداً من المواضيع ذات العلاقة، بما في ذلك الاحتمالات والحساب والإحصاء والتمويل والاقتصاد وبرمجة الحاسوب. ولعل جداول الحياة والوفاة التي تستخدمها شركات التأمين على الحياة هي أشهر تطبيقات هذا العلم. وقد شهد هذا العلم تغيراتٍ ثورية خلال العقود القليلة الماضية مع انتشار الحواسيب فائقة السرعة والدمج الحاصل بين النماذج الاكتوارية مع النظرية المالية الحديثة. واليوم فإن العديد من الجامعات لديها برامج دراسية جامعية وعليا في العلم الاكتواري، خصوصاً وأن بعض الدراسات تشير إلى أهمية وظائف الاكتواريين وتزايد الطلب عليهم في المستقبل، حيث يوجد طلب على هذا التخصص سواء في شركات التأمين والبنوك والمؤسسات المالية ومؤسسات التأمين الاجتماعي والمعاشات وصناديق التقاعد وشركات الاستثمار أو حتى في مجالات لا علاقة لها بالقطاع الاقتصادي والمالي ولكنها تتطلب تقديم تقديرات لحجم المخاطر المحتملة. https://ar. wikipedia. org/wiki

بالعنصرية والتمييز على أساس الجنس والفجوات في الأجور ذات الصلة، ما أثرذلك على الروح المعنوية للموظفين في المؤسسة.

حاولت المؤسسة معالجة المخاوف والانخفاض في الروح المعنوية لموظفيها من خلال إنشاء خط ساخن للموظفين الذين شعروا ''بالتهديد من الإفراج عن المعلومات الشخصية والمالية، وتقديم جلسات استشارية لمعالجة التوتر وعقد لقاءات في قاعة البلدية، وبغض النظر عن هذه الإجراءات، فقد أفاد الموظفون، بعد أشهر من الاختراق، بأنهم شعروا ''بفراغ في القيادة''،

بعد أن تعافت هيئة النقل في جنوب شرق ولاية بنسلفانيا من هجوم سيبراني أدى إلى تعطيل معلومات الحافلات والسكك الحديدية في الوقت الفعلي لمدة أسبوعين، قال أحد الموظفين: ''المعنويات منخفضة حقاً حقاً''.

لم تؤثر الحادثة على الخدمات التي تواجه المستهلك فحسب، بل أثرت أيضاً على وصول الموظفين إلى الخوادم حيث يتم تخزين الملفات والمشاريع ومعلومات الاتصال الضرورية، ترتبط معنويات الموظفين المنخفضة بزيادة التهديدات الخبيثة من الداخل، يمكن للموظفين الساخطين تعطيل العمليات أو حذف البيانات أو نشر بيانات حساسة للعامة لإلحاق الضرر بصاحب العمل.

التأثير على قطاعات حكومية مختارة

تعد الخدمات الحكومية هدفاً مغرياً للجهات الحكومية ومجرمي الإنترنت ونشطاء القرصنة، فالمكسب الاقتصادي يعد حافز مهم، على سبيل المثال، بين آذار 2016 وشباط 2018، حاول ثلاثة مجرمين سيبرانيين نيجيريين، بعد سرقة نماذج ضرائب (W-2) السرية من أكثر من (1200) فرد، المطالبة بحوالي (4 – 16) مليون دولار، لكن يمكن أن يكون لهذه الحوادث آثار أعمق من الخسارة المالية، إذ قد ترقى الانتهاكات إلى حد تهديد الأمن القومي.

تدعي لجنة الطاقة الشمسية للفضاء السيبراني في الولايات المتحدة الامريكية أن ''الولايات المتحدة الامريكية تعمل الآن في مشهد سيبراني يتطلب مستوى من أمن البيانات والمرونة والجدارة بالثقة لا تستطيع الحكومة الأمريكية ولا القطاع الخاص وحده توفيره حالياً، وفضلاً عن ذلك، تتزايد أوجه القصور في المرونة والخبرة الفنية وتوحيد الجهود، سواء داخل الحكومة الأمريكية أو بين القطاعين العام والخاص، بعد اختراق مكتب إدارة شؤون الموظفين، تم تسريب بيانات(SF-86)

[14] لأكثر من(21. 5) مليون فرد، بالإضافة إلى سجلات بصمات الأصابع لـ (5. 6) مليون فرد إضافي، كانت مخاوف الأمن القومي عميقة، حيث حصلت الصين على بيانات حساسة.

أجاب الموظفون الحكوميون على استطلاعنا عموماً بشكل مشابه لتلك الموجودة في القطاعات الأخرى، ومع ذلك، فقد اختلفت ردود أفعالهم عن زملائهم في القطاع الخاص في مجالات قليلة، تبدو الحكومات معرضة بشكل خاص للهجمات الخبيثة من الداخل، ومن الأمور ذات الأهمية وذات الصلة، أشار العديد من المسؤولين الحكوميين أيضاً إلى أن سياسات العاملين عن بُعد و"إحضار جهازك الخاص" (BYOD)[15] تشكل تحديات خاصة بالنسبة لهم، وتسلط ردودهم الضوء أيضاً على المخاوف المتعلقة بنقص المهارات بين موظفي الأمن وصعوبة إدارة المخاطر التي يشكلها استخدام موظفيهم لمنصات التواصل الاجتماعي وخدمات الأعمال الشخصية مثل (Dropbox)[16]، اظهرت البيانات أيضاً أن الوكالات الحكومية أقل احتمالية

14- الانموذج القياسي (SF 86):هو استبيان حكومي أمريكي يكمله الأفراد حتى تتمكن الحكومة من جمع المعلومات من أجل «إجراء تحقيقات في الخلفية وإعادة التحقيق والتقييمات المستمرة للأشخاص قيد النظر في مناصب الأمن القومي **أو** الاحتفاظ بها». يتميز SF 86 عن SF 85، والذي يستخدم للثقة العامة أو المناصب منخفضة المخاطر. يجب إكمال الانموذج من قبل الأفراد العسكريين والمتعاقدين الحكوميين والموظفين الحكوميين من أجل الحصول على التصريح الأمني المطلوب. تتضمن المعلومات المطلوبة في الانموذج أي كليات أو جامعات حضرت على مدار السنوات الثلاث الماضية، وحساب السنوات العشر الأخيرة من عمل الفرد، والعلاقات مع الرعايا الأجانب والحكومات، والسفر إلى الخارج، وقائمة الإقامات السابقة، وما إلى ذلك.

https://en. wikipedia. org/wiki/Standard_Form_86

15- يشير إحضار جهازك الخاص (BYOD) إلى اتجاه الموظفين الذين يستخدمون الأجهزة الشخصية للاتصال بشبكاتهم التنظيمية والوصول إلى الأنظمة المتعلقة بالعمل والبيانات التي يحتمل أن تكون حساسة أو سرية، يمكن أن تشمل الأجهزة الشخصية الهواتف الذكية أو أجهزة الكمبيوتر الشخصية أو الأجهزة اللوحية أو محرك أقراص USB، نظرًا لأن المزيد والمزيد من المؤسسات تدعم الموظفين الذين يعملون من المنزل، أو تحافظ على جدول زمني مرن، أو الاتصال أثناء التنقل أثناء السفر أو التنقل، فقد أصبحت حلول BYOD أكثر انتشاراً. قد تفرض بعض الشركات عقوبات على BYOD، بينما قد تعتبره شركات أخرى جزءاً من «shadow IT»، والتي تشير إلى البرامج أو الأجهزة التي لا تدعمها تقنية المعلومات.

https://www. forcepoint. com/cyber-edu/bring-your-own-device-byod

16- دروبوكس (Dropbox) :هي خدمة استضافة ملفات تديرها شركة دروبوكس الأمريكية، ومقرها في سان فرانسيسكو، كاليفورنيا، والتي توفر التخزين السحابي، ومزامنة الملفات، والسحابة الشخصية وبرامج العميل، كما بالإمكان استعمال الخدمة لتبادل الملفات بين أكثر من مستخدم على الإنترنت ومزامنة الملفات بين أكثر من جهاز حاسوب أو هاتف محمول.

تم تصميم البرنامج عام 2007 من قبل طلاب معهد ماساتشوستس للتكنولوجيا وهما درو هوستون (Drew Houston) وأراش فردوسي (Arash Ferdowsi) كشركة ناشئة، بتمويل أولي من مسرّع بدء التشغيل واي كومبنتر، يقدم البرنامج خدمة استضافة الملفات بطريقتين، الأولى مجانا حتى 2 جيجابايت (بالإمكان زيادتها إلى 18 جيجابايت بشروط معينة) وخدمة مدفوعة تصل إلى 1 تيرابايت، كما يعمل البرنامج تحت 10 أنواع نظم تشغيل للحاسب ومنها ويندوز وماك ولينوكس وسولاريس، بالإضافة

لإشراك إداراتها القانونية في التخطيط للهجمات السيبرانية أو الاستجابة لها مقارنة بأي صناعة أخرى، كما أنها أكثر استعداداً لإغلاق أنظمتها بالكامل كجزء من عملية الاسترداد.

أخيراً، من المرجح أن يتم الكشف علناً عن الهجمات على الأنظمة الحكومية أو الإبلاغ عنها في وسائل الإعلام، ولا ينبغي أن يكون مفاجئاً أن يجد صناع القرار في مجال تكنولوجيا المعلومات في الحكومة الضرر الذي يلحق بالعلامة التجارية أحد التكاليف الخفية التي يواجهونها في مدى أكبر من الصناعات الأخرى، وذلك التأثير له تباين جغرافي، بالنسبة لصانعي القرار في مجال تكنولوجيا المعلومات الحكوميين الذين تمت مقابلتهم، أشار(40%) من الأشخاص في الولايات المتحدة الامريكية إلى الضرر الذي يلحق بالعلامة التجارية باعتباره مصدر قلق مقارنة بـ (28%) من صانعي القرار الحكوميين الآخرين بشأن تكنولوجيا المعلومات، يبدو أيضاً أن القطاع الحكومي في الولايات المتحدة الأمريكية يستغرق وقتاً أطول لتصحيح تأثير حوادث أمن تكنولوجيا المعلومات مقارنة بنظرائهم في البلدان الأخرى والقطاعات الأخرى.

على سبيل المثال، بينما استغرق الأمر، في المتوسط ، 15 ساعة لاكتشاف الحل الوسط الذي أدى إلى أطول حادث لأمن تكنولوجيا المعلومات في عام 2019، أفاد صانعو القرار في مجال تكنولوجيا المعلومات في الحكومة الأمريكية أنهم استغرقوا 17 ساعة لاكتشافه، يمتد هذا الجدول الزمني الأطول إلى خطة الاستجابة، ويستغرق 39 ساعة من الاكتشاف للوصول إلى العلاج و 45 ساعة للوصول إلى التعافي (مقارنة بـ 28 ساعة و 38 ساعة تم الإبلاغ عنها لجميع الذين شملهم الاستطلاع في مجال تكنولوجيا المعلومات).

إلى نظم تشغيل الهواتف المحمولة كالأندرويد والآي أو إس، من أهم منافسيه في هذا المجال: بوكس دوت نت (Box. net) وشوغارسينك (Sugarsync) وموزي (Mozy) وزومو درايف (ZumoDrive) وغيرها.

عند تثبيت برنامج دروبوكس على جهاز الحاسوب سوف يظهر على شكل مجلد يمكن وضعه على سطح المكتب وتتعامل معه كأي مجلد آخر ولكن في الحقيقة هو موجود في سيرفر دروبوكس ولكن صورته لديك. صُنفت دروبوكس كواحدة من أكثر الشركات الناشئة قيمة في الولايات المتحدة والعالم، مع تقييم يزيد عن 10 مليار دولار أمريكي، وقد تم وصفه بأنه أحد أنجح استثمارات واي كومبنتر حتى الآن، ومع ذلك، فقد تعرضت دروبوكس أيضاً لانتقادات وأثارت جدلًا بشأن قضايا مثل الانتهاكات الأمنية ومخاوف الخصوصية، فقد تم حظر دروبوكس في الصين منذ عام 2014. توفر الخدمة العديد من اللغات حيث بلغ عددها 22 لغة: الصينية (التقليدية والمبسطة) والإنجليزية (الأمريكية والبريطانية) والفرنسية والألمانية والإندونيسية والإيطالية والكورية والماليزية والبولندية والبرتغالية (البرتغالية والبرازيلية) والروسية والإسبانية (القشتالية وأمريكا اللاتينية) والأوكرانية. حازت الخدمة على العديد من الجوائز من قبل المواقع التقنية، وحصلت على تصنيف خمس نجوم في تقرير»حماية بياناتك من الطلبات الحكومية» الصادر عن مؤسسة الحدود الإلكترونية لعام 2017، كما أشادت بها عدة صحف عالمية. https://ar. wikipedia. org/wiki

وجد الاستطلاع الذي أجريناه أن صانعي القرار في مجال تكنولوجيا المعلومات في الحكومة أقل ابلاغ عن خروقات البيانات التي تمثل أعلى تكلفة لمؤسساتهم، من المرجح أن يتم تعليل ذلكبانهجمات رانسوم وير(برنامج الفيدية)[17]، والتصيد الاحتيالي، والهجمات الخبيثة من الداخل تمثل أعلى تكلفة من الهجمات الاخرى، قد يعكس هذا النتيجة غير المقصودة لقانون إدارة أمن المعلومات الفيدرالي FISMA))[18] بموجب هذا القانون، قد يتم تحفيز الوكالات الفيدرالية عن غير قصد للإبلاغ عن الحوادث الأمنية بطريقة لا تضر بدرجة الامتثال للقانون الفيدرالي لإدارة أمن المعلومات (FISMA).

17- رانسوم وير عبارة عن هجوم إلكتروني (فيروس): يُستخدم لابتزاز المستخدم وتحريضه على دفع المال. كان المجرمون في البداية يستخدمون رانسوم وير كوسيلة ابتزاز لجني الأموال من الأفراد الذين يريدون استرداد معلوماتهم الشخصية. واليوم يستخدم المجرمون رانسوم وير كوسيلة ابتزاز لجني الأموال من الشركات التي تريد استرداد معلوماتها الحساسة، لا يوجد جهاز محصّن من رانسوم وير، فقد ابتز المجرمون الأفراد لتحريضهم على دفع الأموال مقابل استرداد معلوماتهم الشخصية أو الطبية من مزوّدي الرعاية الصحية ومنعوا الضيوف من الدخول إلى غرفهم في الفنادق، حتى أن الأنظمة الصناعية أثبتت حساسيّتها اتجاه فيروس رانسوم وير، كان فيروس رانسوم وير في السابق يمنع الضحية من الوصول إلى سطح مكتبه أو متصفّح الإنترنت الخاص به، ثم بدأ مهاجمو الإنترنت يستخدمون برنامج رانسوم وير – السرّي الأكثر تعقيدًا لتشفير المعلومات على أجهزة الحاسوب أو الهواتف المحمولة، ويرسل كلا البرنامجين إشعار ابتزاز إلى المستخدم: اشتري برنامج فك التشفير أو مفتاح فك التشفير أو ستخسر بياناتك للأبد.

https://www. icann. org/ar/blogs/details/what-is-ransomware-13-3-2017-ar

18- قانون إدارة أمن المعلومات الفيدرالي (FISMA): هو قانون فيدرالي أمريكي تم تمريره في عام 2002 والذي جعل من المطلوب من الوكالات الفيدرالية تطوير وتوثيق وتنفيذ برنامج لأمن وحماية المعلومات، والقانون هو جزء من قانون الحكومة الإلكترونية الأكبر لعام 2002 الذي تم تقديمه لتحسين إدارة خدمات وعمليات الحكومة الإلكترونية، القانون الفيدرالي لإدارة أمن المعلومات (FISMA) هو أحد أهم اللوائح الخاصة بمعايير وإرشادات أمان البيانات الفيدرالية، تم تقديمه لتقليل المخاطر الأمنية على المعلومات والبيانات الفيدرالية أثناء إدارة الإنفاق الفيدرالي على أمن المعلومات، لتحقيق هذه الأهداف، أنشأ القانون الفيدرالي لإدارة أمن المعلومات (FISMA) مجموعة من الإرشادات ومعايير الأمان التي يتعين على الوكالات الفيدرالية الوفاء بها. وقد توسع نطاق القانون الفيدرالي لإدارة أمن المعلومات (FISMA) منذ ذلك الحين ليشمل الوكالات الحكومية التي تدير البرامج الفيدرالية مثل ميديكير، تنطبق متطلبات القانون الفيدرالي لإدارة أمن المعلومات (FISMA) أيضًا على أي شركة خاصة تشارك في علاقة تعاقدية مع الحكومة، في أبريل 2010، أصدر مكتب الإدارة والميزانية (OMB) إرشادات تتطلب من الوكالات تقديم معلومات نظام في الوقت الفعلي إلى مدققي FISMA، مما يتيح المراقبة المستمرة لأنظمة المعلومات الخاضعة للوائح FISMA.

Nate Lord، What is FISMA Compliance? 2019 FISMA Definition، Requirements، Penalties، and More، Tuesday December 1، 2020، https:// digitalguardian. com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more.

العناية الصحية:

غالباً ما تحتوي السجلات الطبية على تفاصيل مالية وأرقام ضمان اجتماعي بالإضافة إلى معلومات صحية سرية وحساسة، ما يجعل القطاع الصحي هدفاً جذاباً بشكل خاص لمجرمي الإنترنت، غالباً ما تعتمد المستشفيات أيضاً على أنظمة مؤمنة بشكل سيئ وحيوية لعملياتها، لذلك كان قطاع الرعاية الصحية هدفًا ناضجاً للجرائم السيبرانية، أصبحت هجمات برامج الفدية على المستشفيات أمراً شائعاً، مع وجود هجمات منتظمة في جميع أنحاء العالم –من فرنسا إلى أستراليا– وخاصة في الولايات المتحدة الامريكية.

في هجوم أنموذجي، يتم حظر المستشفيات متوسطة الحجم ذات موارد تكنولوجيا المعلومات المحدودة من أنظمتها وإجبارها على دفع فدية يمكن أن تتراوح من آلاف الدولارات إلى الملايين. هذه المبالغ تضيف تكلفة بالتأكيد، لكن الآثار الأكثر تكلفة للجرائم السيبرانية على قطاع الرعاية الصحية جاءت من هجمات أوسع نطاقاً لم تميز بين أهدافها.

أثر هجوم (WannaCry[19]) في العام 2017 على مئات الآلاف من أجهزة الكمبيوتر ولكنه كان محزناً بشكل خاص لنظام الصحة الوطني في المملكة المتحدةالبريطانية (NHS)[20]، إذ اضطرت هيئة الخدمات الصحية الوطنية (NHS) إلى إيقاف تشغيل أكثر من ثلث أنظمتها، إما لأنها قد تأثرت وإما لأنها كانت في خطر، مما أدى إلى تباطؤ الأداء بشكل كبير وأثر على رعاية

19–هجوم واناكراي السيبراني أو ما يعرف بهجوم WannaCrypt أو Wannacrypt0r 2. 0: هو هجوم ببرمجية الفدية بدأ في الساعات الأولى من يوم 12 مايو 2017 واستطاع الإطاحة بأكثر من 230 ألف جهاز إلكتروني في 99 دولة حول العالم حسب اليوروبول. تقوم البرمجية بتشفير جميع البيانات الموجودة على الحاسوب، فيما تظهر رسالة متوفرة بـ 28 لغة تفيد بأن عليك دفع مبلغ 300 دولار مقابل الإفراج عن بياناتك المشفرة، يستغل فيروس الفدية ثغرة شديدة في بروتوكول SMB تعرف بـ MS17- 010، لذا قامت شركة مايكروسوفت بإصدار تحديث خاص لها في منتصف شهر مارس 2017. في النصف الثاني من شهر يونيو (حزيران) 2017، عاد فيروس الفدية من جديد بنسخة جديدة تم تطويرها لتفادي الثغرة الموجودة في النسخة الأولى والتي تتمثل في اسم نطاق الذي يقوم بإيقافها عن العمل، تلك الثغرة التي استفاد منها ماركوس هاتشينز لإيقاف البرمجية.
https://ar. wikipedia. org/wiki

20– هيئة الخدمات الصحية الوطنية (National Health System): وتختصر NHS «إن إتش إس» هي نظام تقديم الخدمات الصحية للمواطنين في إنكلترا وهو ممول من قبل القطاع العام، ويجب عدم خلطها مع أجهزة الصحة الوطنية الثلاثة الأخرى التي تعمل عبر المملكة المتحدة في مقاطعاتها الخاصة ضمن حكوماتها الخاصة والتي طورت قوانين تختلف بعض الشيء عن بعضها البعض، أجهزة الخدمات الأربع تقدم خدمات من دون اختلاف في الحقوق لمواطني المقاطعات الأخرى كمقاطعاتهم، حالياً، توظف الNHS حوالي 1. 33 مليون شخص، والذي يجلعها رابع أكبر عدد من الموظفين بعد الجيش الصيني، وخطوط سكك الحديد الهندية، وسلسلة وول مارت، عدد الموظفين الذين يعملون بكامل الوقت هم 980. 000 شخص:
https://ar. wikipedia. org/wiki

المرضى في العديد من مرافق الرعاية الصحية، على الرغم من أن هجوم (WannaCry) لم يؤد إلى أي وفيات، إلا أنه تسبب في إلغاء أكثر من (19000) موعداً طبياً، وتم تقدير تكاليف الإنتاجية المفقودة وجهود استعادة النظام وترقيات تكنولوجيا المعلومات لخدمة الصحة الوطنية (NHS) بمبلغ (92) مليون جنيه إسترليني.

كان هجوم (NotPetya) أيضاً مكلفة للغاية بالنسبة لقطاع الرعاية الصحية إذ أصاب الهجوم المستشفيات الأوكرانية بالشلل، في قطاع الرعاية الصحية التجارية، تكبدت شركة الأدوية العملاقة (Merck) في النهاية خسائر قد تتجاوز مليار دولار، وانتشر الفيروس أيضاً من (Merck) إلى أجزاء أخرى من سلسلة التوريد الدوائية وتسبب في تأخير تسليم الأدوية الموصوفة في جميع أنحاء العالم، تعد دراسة حالة شركة (Breach Anthem)[21]، في العام 2015 دراسة أخرى مثيرة للاهتمام، إذ تم سرقة ما يقرب من مليون سجل في اثناء عملية الخرق، وانتهى الأمر بشركة التأمين بإنفاق (2، 5) مليون دولار على الاستشاريين، و(115) مليون دولار على التحسينات الأمنية، و(31) مليون دولار لإعلام المستهلكين، و (112) مليون دولار لحماية الائتمان للمتضررين من الانتهاك، كانت هجمات (NotPetya) و(WannaCry)) وخرق (Anthem) من بين الهجمات الفردية الأكثر ضرراً على قطاع الرعاية الصحية، ويبدو أن الجهات الحكومية قد تكون مسؤولة عن كل منهما، مما يثير تساؤلات حول القانون الدولي والمعايير التي تحمي أنظمة الرعاية الصحية.

21-ان خرق البيانات الطبية لشركة Anthem بمثابة خرق للبيانات الطبية للمعلومات التي تحتفظ بها شركة Anthem Inc، في 4 شباط 2015، كشفت شركة Anthem، Inc، أن المتسللين المجرمين قد اخترقوا خوادمها ومن المحتمل أن يكونوا قد سرقوا أكثر من (37، 5) مليون سجل تحتوي على معلومات تعريف شخصية من خوادمها. في 24 شباط 2015، رفعت Anthem العدد إلى (78، 8) مليون شخص تأثرت معلوماتهم الشخصية. وفقاً لشركة Anthem، Inc. ، امتد خرق البيانات ليشمل العديد من العلامات التجارية التي تستخدمها Anthem، Inc. لتسويق خطط الرعاية الصحية، بما في ذلك Anthem Blue Cross و Anthem Blue Cross و Blue Shield و Blue Cross و Blue Shield of Georgia و Empire بلو كروس وبلو شيلد، أميريجروب، كارمور، ويوني كير. تقول Healthlink أنها كانت أيضًا ضحية. يقول Anthem إن المعلومات الطبية والبيانات المالية للمستخدمين لم يتم اختراقها. عرضت Anthem مراقبة ائتمانية مجانية في أعقاب الخرق. وفقًا لـ Bloomberg News، قد تكون الصين مسؤولة عن هذا الخرق للبيانات. قال مايكل دانيال، كبير مستشاري الأمن السيبراني للرئيس باراك أوباما، إنه سيغير كلمة المرور الخاصة به. وفقًا لصحيفة نيويورك تايمز، تم اختراق حوالي 80 مليون سجل للشركة، وهناك خوف من استخدام البيانات المسروقة لسرقة الهوية. احتوت المعلومات المخترقة على الأسماء وأعياد الميلاد والمعرفات الطبية وأرقام الضمان الاجتماعي وعناوين الشوارع وعناوين البريد الإلكتروني ومعلومات التوظيف، بما في ذلك بيانات الدخل:https://en. wikipedia. org/wiki/Anthem_medical_data_breach

زادت الهجمات أيضاً خلال أزمة فيروس كورونا، مع استفادة الجهات الفاعلة الخاصة والحكومية من الظروف للاحتيال على الضحايا وسحب البيانات من الباحثين، وقد أدى ذلك إلى دعوات جديدة لإعلان حظر أنظمة الرعاية الصحية، بما في ذلك الاتحاد الأوروبي (بيان أكسفورد)، لكن يبدو أن هذا القطاع سيظل ضعيفاً، في حزيران 2020، أصدر مكتب التحقيقات الفيدرالي ''تنبيهاً سريعاً للمالية والرعاية الصحية والصناعات الكيماوية في الولايات المتحدة التي تدير أعمالاً تجارية في الصين حول الاستهداف المحتمل من قبل الحكومة الصينية عبر برنامج الضرائب الذي تفرضه الدولة، وفقًا لمكتب التحقيقات الفيدرالي، فإن شركتي (Baiwang) و(Aisino) هما فقط تقدمان خدمات البرمجيات الضريبية المرخص لهما من الحكومة وفقاً لضريبة القيمة المضافة المنقحة في الصين في العام 2018، البرنامج الضار المضمن في برامج الضرائب الإلزامية، والذي سمي أحدها على نحو مناسب باسم ''ضريبة الاستخبارات''، ممكنه بشكل أساسي من الدخول إلى شبكات الضحايا والأنظمة التي تستخدم البرامج الضارة، أفاد مكتب التحقيقات الفيدرالي (FBI) أن هذه الثغرة الأمنية على الأرجح قد منحت الجهات الفاعلة الإلكترونيةقدرة الوصول إلى ''إجراء تنفيذ التعليمات البرمجية عن بُعد وأنشطة التسلل على شبكة الضحية''.

من غير المعروف عدد الشركات التي تم اختراقها، والتي تستخدم خدمات البريد الإلكتروني المستندة إلى السحابة، لا سيما في قطاعي المال والأعمال، هي أهداف مربحة لمجرمي الإنترنت الذين يجرون عمليات احتيال البريد الإلكتروني التجارية (BEC)، وفقاً لـ(IC3)(مركز شكاوى جرائم الانترنت) التابع لمكتب التحقيقات الفيدرالي، كانت هنالك زيادة مطردة في عمليات الاحتيال (BEC) منذ 2014 ومن 2014 إلى 2019، تلقى مركز شكاوى جرائم الإنترنت (IC3) ''شكاوى يبلغ مجموعها أكثر من (2. 1) مليار دولار خسائر لفعلية من عمليات الاحتيال (BEC) التي تستهدف أكبر المنصات''.

هذا مهم لأنه يسلط الضوء على أن عمليات الاحتيال ((BEC التي تتزايد في الحجم وأن المستخدمين يكافحون للحفاظ على أمان حساباتهم. نظراً لأن المزيد من الموظفين يتجهون إلى العمل عن بُعد على الأجهزة الشخصية وأجهزة الشركة أثناء (COVID-19)، بالإضافة إلى إجراء المعاملات المالية الافتراضية، فقد يخلق ذلك بيئة أكثر خصوبة لعمليات التصيد الاحتيالي (BEC) التي تستهدف القطاع المالي، ينجذب مجرمو الإنترنت بشكل طبيعي إلى القطاع المالي، حيث يوجد المال.

إن حدوث عدد أقل من النجاحات الدراماتيكية هو تقدير للجهود المكثفة التي بذلها القطاع في مجال الأمن السيبراني في كل من المؤسسات الفردية والجماعية، ومع ذلك، فإن هذا يأتي بتكلفة تصل إلى (3000) دولار لكل موظف على الأمن السيبراني، وجدت دراسة استقصائية أجراها (ISAC-FS)[22] في 2018 أن المؤسسات المالية تنفق (حسب حجمها) ما بين (6% - 14%) من ميزانيات تكنولوجيا المعلومات للدفاع حيث بلغ الإنفاق العالمي على الأمن السيبراني ما يقرب من (145) مليار دولار في عام 2019.

بالإضافة إلى خسائرنا المقدرة البالغة (945) مليار دولار، وتحول الجريمة السيبرانية إلى عبء يزيد على تريليون دولار في الاقتصاد العالمي، لا يتم توزيع المخاطر بالتساوي، ولا تتعرض بعض الشركات لخسائر بينما يخسر البعض الآخر الملايين، الأمر المثير للقلق هو أن عدداً أقل من الشركات يمكنها القول إنها لن تتعرض أبداً لقرصنة ضارة، تنجو بعض الشركات من الخسارة، بينما تتضرر شركات أخرى، وهذا يعزز الحاجة إلى التخطيط المناسب للهجمات السيبرانية، وعلى الرغم من حقيقة أن الوقوع ضحية للجرائم السيبرانية هو أمر يتعلق بالوقت أكثر مما إذا كان هناك الكثير الذي يمكن للمؤسسات القيام به للمساعدة في منع حوادث أمن تكنولوجيا المعلومات أو تقليل الضرر والتأثير على المؤسسة، بالكاد يوجد تقرير عن الأمن السيبراني لا يختتم بتوصيات للمؤسسات لتحسين الامن السيبراني وتنفيذ أفضل الممارسات المعروفة، تتضمن بعض أفضل الممارسات ما يلي:

1. التنفيذ الموحد للتدابير الأمنية الأساسية.

2. زيادة الشفافية داخل المنظمات.

3. توحيد وتنسيق متطلبات الأمن السيبراني. 4. توفير تدريب توعية بالأمن السيبراني للموظفين.

22- Financial Services Information Sharing and Analysis Center: عد مركز تبادل وتحليل معلومات الخدمات المالية (FS-ISAC) اتحادًا صناعيًا مخصصًا لتقليل المخاطر الإلكترونية في النظام المالي العالمي. من خلال خدمة المؤسسات المالية وعملائها بدورها، تستفيد المؤسسة من نظامها الاستخباري وموارد المرونة وشبكة خبراء موثوق بها من نظير إلى نظير لتوقع التهديدات السيبرانية والتخفيف من حدتها والاستجابة لها. FS-ISAC لديها ما يقرب من 7000 شركة عضو مع مستخدمين في أكثر من 70 دولة. يقع المقر الرئيسي للمنظمة في الولايات المتحدة، ولها مكاتب في المملكة المتحدة وسنغافورة.

https://en. wikipedia. org/wiki/Financial_Services_Information_Sharing_and_Analysis_Center

5. تطوير خطط الوقاية والاستجابة.

نشر مركز الدراسات الاستراتيجية والدولية (CSIS) عدة تقارير حول كيفية قيام المؤسسات بحماية نفسها بشكل أفضل، على الرغم من أن بعض التقارير تعود إلى عدة سنوات، إلا أن التوصيات ما تزال سارية، يعد تنفيذ تدابير الأمن السيبراني البسيطة، مثل المصادقة متعددة العوامل والنسخ الاحتياطي أمراً ضرورياً ويقطع شوطاً طويلاً نحو تقليل العديد من الخسائر الناجمة عن الجرائم السيبرانية.

يقدم تقرير استشاري صدر مؤخراً بالاشتراك من سلطات الأمن السيبراني في أستراليا وكندا ونيوزيلندا والمملكة المتحدة والولايات المتحدة الامريكية توصياتهم الجماعية للمؤسسات لتجنب الأخطاء التقنية الشائعة عند الاستجابة لأول مرة لحادث السيبراني، لكن تنفيذ الحلول التقنية لن يحل جميع المشكلات، أسفر المسح الذي أجريناه عن نتائج تتعلق ببعض الصعوبات التي تواجهها المؤسسات داخلياً والتي تساهم في جعلها أكثر عرضة للهجمات السيبرانية، على سبيل المثال، اعتبر(507) من أصل (1332) مشاركاً أن نقص معرفة المستخدم ساهم في نجاح مجرمي الإنترنت الذين يستهدفون مؤسساتهم، يتمثل أحد أكبر التحديات في الافتقار إلى فهم على مستوى المؤسسة للمخاطر السيبرالية، يجعل هذا الشركات والوكالات عرضة لأساليب الهندسة الاجتماعية، بمجرد اختراق المستخدم، لا يتعرف دائماً على المشكلة في الوقت المناسب لوقف انتشار البرامج الضارة.

ويؤدي الاستخدام المتزايد (والذي لا مفر منه) للأجهزة الشخصية مثل الهواتف الذكية أو الأجهزة اللوحية إلى توسيع سطح الهجوم ونقاط النهاية للهجوم وتعقيد إدارة الدفاع السيبراني، هنالك وجه آخر لهذا الانفصال يتعلق بكيفية استجابة الشركات بعد وقوع حادث، كما ذكرنا سابقًا، قال (38%) من المستطلعين إن نقص معرفة المستخدم كان السبب لنجاح الهجمات، ومع ذلك، كان الاستثمار في برامج جديدة أو مختلفة هو التعديل الأكثر شيوعاً للعمليات بعد وقوع حادث أمني، رد فعل هذا مفهوم، لكنه في حد ذاته ليس كافياً.

وضع خطط الوقاية والاستجابة.

ليس من المستغرب أن يكون ضمان وجود خطة قائمة لمنع حوادث أمن تكنولوجيا المعلومات والاستجابة لها تحت ادارة واحدة أمراً أساسياً للنجاح عندما يحين الوقت، ومع ذلك، قال (44%) فقط من المشاركين في الاستطلاع بأنهم كان لديهم خطط لمنع حوادث أمن تكنولوجيا المعلومات

والاستجابة لها، واشار (32%) من صانعي القرار إن لدى مؤسساتهم خطة لمنع حوادث أمن تكنولوجيا المعلومات، إلا أنهم لا يبدون اهتماماً بموضوع الاستعداد للاستجابة، حيث صرح (19%) فقط بوجود خطة استجابة، علاوة على ذلك.

لم يتم اعتبار هذه الخطط مفيدة أو ناجحة، إذ وجد (32%) فقط من المشاركين أن خطط مؤسساتهم ناجحة تماماً في الاستجابة لحوادث أمن تكنولوجيا المعلومات، وعلى الرغم من أن معظمهم (62%) يعتبرون ''ناجحين إلى حد ما''، إلا أن هنالك مجالًا لتحسين قلة التواصل داخل المؤسسة، تواجهالمؤسسات التي لديها خطط لمنع أو الاستجابة لحوادث أمن تكنولوجيا المعلومات مشكلة الاتصال، فعلى الرغم من أنه من الضروري أن يكون هنالك تداخل بين أولئك الذين يضعون الخطة والذين يشاركون في الاستجابة الفعلية، إلا أن التواصل عبر المؤسسة وأصحاب المصالح المختلفين ذوي الصلة ضروري أيضاً.

يمتلك صانعو القرار في مجال تكنولوجيا المعلومات والأعمال (LOB) فهماً مختلفاً لما ولماذا وكيف تتعرض شركة أو وكالة حكومية لحادث أمن تكنولوجيا المعلومات، من المحتمل أن يكون هذا بسبب عدم وجود رؤية للمديرين التنفيذيين في (LOB)[23] بشأن ما يحدث، ولايوجد تواصل كافي عبر الأقسام، تشير الأرقام إلى أن صانعي القرار (LOB) يعتقدون أن هناك خططاً للاستجابة للحوادث في حين أنه في الواقع قد لا يكون هنالك، في حين أن (42%) من صانعي القرار في مجال تكنولوجيا المعلومات يقولون إن كليهما موجود، أجاب (47%) من صانعي القرار في (LOB) بشكل إيجابي على السؤال نفسه.

ليس من المستغرب أن يكون المدراء التنفيذيون في أقسام تكنولوجيا المعلومات أكثر وعياً بعدد التحقيقات التي تم إجراؤها، في حين لم يعرف (18%) من صانعي القرار في (LOB) عدد التحقيقات التي تم إجراؤها، عندما يتعلق الأمر بتأثير هجمات الفدية أو هجمات (DoS /

23- نوع النشاط (LOB) :هو مصطلح عام يشير إلى مجموعة من واحد أو أكثر من المنتجات وثيقة الصلة ببعضها، والتي تخدم قطاعاً معيناً من صفقات العملاء أو حاجة تجارية، ففي بعض القطاعات الصناعية، مثل التأمين، فإن «نوع النشاط» له تعريف محاسبي وتشريعي يدل على مجموعة قانونية من وثائق التأمين. وقد يمثل نوع النشاط وحدة أعمال وثيقة الصلة من الناحية الإستراتيجية، أو قد لا يكون كذلك. عادةً ما يشير المصطلح «نوع النشاط» إلى وحدة أعمال داخلية في مؤسسة، بينما يشير مصطلح «الصناعة» إلى الصورة الخارجية التي تشمل كل المنافسين الموجودين في أسواق مشابهة. وغالباً، ما يتم تحديد موقع أو مكانة نوع النشاط في أي صناعة باستخدام تحليل القوى الخمس لمايكل بورتر، أو غيره من طرق التحليل الصناعي والتصنيفات الصناعية ذات الصلة: https://ar. wikipedia. org/wiki/

DdoS)[24]، يبدو أن صانعي قرار LOB)) يفتقرون إلى رؤية تأثيرها الفعلي على مؤسساتهم، على عكس التقييم الذي أجراه مديرو تكنولوجيا المعلومات.

المبادرات التي اتخذت بعد حادث خطير تسلط الضوء على أهمية هذه المخاوف. بعد ثلاثة سنوات من خرق شركة (Equifax)، عكسكبير مسؤولي امن المعلومات (CISO)[25] في الشركة أن معالجة مشكلات الاتصال مع (suite-C)[26] وتحسين ثقافة الوعي بالأمن السيبراني للشركة كانا من أكثر التدابير ذات الصلة التي تم وضعها، يفترض انيفهم صناع القرار في تكنولوجيا المعلوماتو (LOB) الثغرات الأمنية التي يمكن أن تؤدي إلى هجمات سيبرانية ناجحة، يرى

24-هجمات الحرمان من الخدمات أو هجوم حجب الخدمة (Denial of Service Attacks) :هي هجمات تتم عن طريق إغراق المواقع بسيل من البيانات غير اللازمة يتم إرسالها عن طريق أجهزة مصابة ببرامج(في هذه الحالة تسمى DDOS Attacks) تعمل نشر هذه الهجمات بحيث يتحكم فيها القراصنة والعابثين الإلكترونيين لمهاجمة الشبكة (الإنترنت)عن بعد بإرسال تلك البيانات إلى المواقع بشكل كثيف مما يسبب بطء الخدمات أو زحاماً مرورياً بهذه المواقع ويسبب صعوبة وصول المستخدمين لها نظراً لهذا الاكتظاظ، خصوصاً وأنه يبدو، وباعتراف الكثير من خبراء الأمن على الشبكة، وكأنه لا يوجد علاج في الوقت الحالي لهذا الأسلوب في الهجوم على مواقع الشبكة (الإنترنت)، وعلى هذا الأساس فإن هذا النوع من الهجمات يُدعى في بعض الأوساط «بإيدز الإنترنت».

يتم هذا الهجوم بدون كسر ملفات كلمات السر أو سرقة البيانات السرية، هجمات حجب الخدمة تتم ببساطه بان يقوم المهاجم بإطلاق أحد البرامج التي تزحم المرور للموقع الخاص بك وبالتالي تمنع أي مستخدم آخر من الوصول إليه، تشير العديد من التقارير إلى تزايد عدد الهجمات من خلال الشبكة (الإنترنت) وازدياد شدتها وتأثيرها التدميري عاماً بعد الآخر وتأثيرها على مبيعات المواقع والخدمات عبر الشبكة، ويرجع ذلك إلى عدة أسباب من أخطرها ما يعرف بـ»هجمات الحرمان من الخدمات» أو «هجمات حجب الخدمة» (Denial of Service Attacks) مختصرة بعبارة /DoS:https://ar. wikipedia. org/wiki

25- كبير مسؤولي أمن المعلومات (CISO) :هو المسؤول التنفيذي رفيع المستوى داخل منظمة مسؤولة عن إنشاء والحفاظ على رؤية المؤسسة واستراتيجيتها وبرنامجها لضمان حماية أصول وتقنيات المعلومات بشكل مناسب، يقوم رئيس أمن المعلومات (CISO) بتوجيه الموظفين في تحديد العمليات وتطويرها وتنفيذها وصيانتها عبر المؤسسة لتقليل مخاطر تكنولوجيا المعلومات والمعلومات، إنهم يستجيبون للحوادث، ويضعون المعايير والضوابط المناسبة، ويديرون تقنيات الأمن، ويوجهون إنشاء وتنفيذ السياسات والإجراءات.

عادةً ما يكون CISO مسؤولاً أيضاً عن الامتثال المتعلق بالمعلومات (على سبيل المثال، الإشراف على التنفيذ لتحقيق شهادة ISO / IEC 27001 لكيان أو جزء منه)، كما أن CISO مسؤول أيضاً عن حماية معلومات الملكية وأصول الشركة، بما في ذلك بيانات العملاء والمستهلكين، يعمل CISO مع المديرين التنفيذيين الآخرين للتأكد من نمو الشركة بطريقة مسؤولة وأخلاقية.

https://en. wikipedia. org/wiki/Chief_information_security_officer

26-C-suite، أو C-level، هي لغة عامية مستخدمة على نطاق واسع تصف مجموعة من كبار المديرين التنفيذيين في الشركة. يحصل C-suite على اسمه من ألقاب كبار المديرين التنفيذيين، والتي تميل إلى البدء بالحرف C، لـ «CEO»، كما هو الحال في الرئيس التنفيذي (CEO)، والمدير المالي (CFO)، ورئيس العمليات (COO)، ورئيس قسم المعلومات (.(CIO
asp .https://www. investopedia. com/terms/c/c-suite

المسؤولون التنفيذيون في (LOB) مخاطر أقل في العمل عن بُعد، أو سياسات BYOD))، أو الاستخدام المتزايد للهواتف الذكية والأجهزة اللوحية –كل الأشياء التي تزيد من سطح الهجوم– مقارنة بنظرائها في مجال تقنية المعلومات.

كذلك أشار المجيبون على الاستطلاع إلى أن نقص معرفة المستخدم سمح للمتطفل بالنجاح، ما يؤكد أهمية جهود محو الأمية الرقمية لجميع الموظفين، على الرغم من أن كبار الموظفين في قسم تكنولوجيا المعلومات يشاركون عادةً في تطوير الخطط (50%) من المشاركين في الاستطلاع شاركوا فيها مشرفي تكنولوجيا المعلومات، و (45%) من مديري تكنولوجيا المعلومات، كان الأمر مقلقاً أن (22%) فقط شاركوا من قسم العمليات و(18%) فقط من القسم القانوني في تخطيط الاستجابة، حدثت مشاركة (suite-C) ومجلس الإدارة في أقل من (36%) من الحالات.

توضح القائمة الطويلة للتكاليف المخفية أن التعاون والتواصل بين الإدارات ضروري، وأن إعلام المناطق الأخرى بالحوادث الجارية ووضع خطة مشاركة لأصحاب المصلحة المتعددين يتيح إدارة أفضل للمخاطر والأزمات، يمتد هذا النقص في التواصل إلى وقت الاستجابة للحوادث أيضاً.

هنالك أقسام لم يتم إخطارها بحدوث حادث سيبراني، ادعى (24%) من صانعي القرار في (LOB) أن إداراتهم تتأثر بشكل مباشر بحادث أمن تكنولوجيا المعلومات، وإذا لم يكونوا على دراية بأسباب تعرضهم لهذه الحوادث، فقد يؤدي ذلك إلى حدوث ارتباك عبر الأقسام، نظراً لأن قلة معرفة المستخدم هي السبب الجذري لنجاح العديد من هذه الحوادث، فإن الاتصال بين الإدارات يعد أمراً أساسياً لضمان إدراكهم وفهمهم للأسباب، فضلاً عن التدابير الوقائية التي يمكن وضعها في مكانها الصحيح.

الملحق أ: الجرائم السيبرانية وازمة كورونا.

وفرت أزمة (COVID-19) بيئة خصبة للجرائم السيبرانية، لم يكن الفاعلون الإجراميون قادرين على تعديل مخططاتهم بسرعة استجابة للوباء فحسب، بل استفادوا أيضاً من الاعتماد السريععلى البنية التحتية للوصول عن بُعد للعمل والتعليم. أصبحت المخططات التقليدية "ذات طابع (COVID-19). يمثل هذا أكبر قدر من النشاط المبلغ عنه في عام 2020 ويتضمن إعداد المجالات الخبيثة والبريد العشوائي وحملات التصيد الاحتيالي وتنفيذ مخططات الاحتيال إما لسرقة بيانات الاعتماد وإما نشر البرامج الضارة وإما الوصول إلى معلومات تحديد الهوية الشخصية.

استهداف المنظمات المحلية والدولية العاملة على الاستجابة للجائحة، تهدف هذه الأنواع من الهجمات في المقام الأول إلى "جمع المعلومات الشخصية والملكية الفكرية في الولايات المتحدةالامريكية، أفاد مسؤولون من (IC3) التابع لمكتب التحقيقات الفيدرالي (FBI) أنه خلال الوباء، زادت شكاوى الجرائم السيبرانية من (1000 إلى 3000 إلى4000) يومياً -بدءاً من شهر اذار، كانت هنالك زيادة حادة في عدد المجالات التي تم تسجيلها والتي تشير إلى فيروس كورونا- على الرغم من أن الزيادة شملت كلاً من المجالات الخبيثة والحميدة، إلا أن المجالات عالية الخطورة تجاوزت (5000) في اليوم خلال شهر اذار، في حين أن المجالات منخفضة الخطورة لم تتجاوز (1000). بدأ هذا الاتجاه في المجالات المتعلقة بـ (COVID-19) في الانخفاض مع تضاؤل الأحداث وعدم اليقين المرتبطين بالأزمة.

بحلول نهاية أيار، وجد استشاري لجنة مكافحة الإرهاب أن تسجيل المجالات الخبيثة المتعلقة بـ (COVID-19) كان أقل من (1000) في اليوم واستمر في اتجاهه التنازلي، قبل (COVID-19)، تلقى (IC3) أكثر من (1200) شكوى يومياً من الضحايا في المتوسط وحوالي (340. 000) شكوى سنوياً في المتوسط على مدى السنوات الخمس الماضية - لم يزد هذا الرقم إلا منذ الوباء حيث بدأ المزيد من مجرمي الإنترنت في استهداف كبار السن وقطاع الرعاية الصحية والمؤسسات المالية والمؤسسات الحكومية وبرامج التحفيز وحماية الراتب—وذكرت اللجنة القضائية بمجلس الشيوخ في حزيران 2020 أنه: ابتداءاً من 28 ايار 2020، تلقى مركز شكاوى جرائم الإنترنت (IC3) فيها تقريباً نفس عدد الشكاوى في عام 2020 (حوالي 320. 000) كما كان في عام 2019 بأكمله (حوالي 400. 000) - ما يقرب من (75%) من هذه الشكاوى عبارة عن عمليات احتيال ونصب، ما يمثل تحدياً للبرنامج الإجرامي لمكتب التحقيقات الفيدرالي نظراً للحجم الهائل من الطلبات، تتضح هذه الزيادة في نشاط الجرائم السيبرانية خلال (COVID-19) أيضاً في تقرير خدمة التصفح الآمن من Google، والذي أشار إلى زيادة مطردة في مقدار مواقع التصيد الاحتيالي -هذه صفحات ويب المزيفة تحاول خداع المستخدمين لمشاركة معلومات خاصة مثل أسماء المستخدمين وكلمات المرور والمعلومات المصرفية من خلال الظهور على أنها مواقع ويب شرعية- وفقاً لتقرير شفافية التصفح الآمن من Google على مواقع الويب غير الآمنة، في نهاية شباط 2020، اكتشفتGoogle (1. 690. 000) موقع تصيد، وبحلول نهاية شباط، ارتفع هذا الرقم إلى (000، 695، 1)، ثم إلى(244، 798، 1) بنهاية آذار ونيسان ولم يظهر أي علامة على التوقف حيث تضخم عدد مواقع التصيد إلى ما يقرب

من (1، 900، 000)، مع انتقال المؤسسات إلى العمل عن بُعد استجابةً لإرشادات الرعاية الصحية، احتاجوا إلى نشر تقنيات جديدة للوصول عن بُعد والبنية التحتية للعمل عن بُعد، سمحت هذه الخطوة باستغلال نقاط الضعف التي لم تكن موجودة من قبل.

توقع مكتب التحقيقات الفيدرالي في أوائل نيسان أن مجرمي الإنترنت سيحاولون الاستفادة من ''الاستخدام المتزايد للبيئات الافتراضية من قبل الوكالات الحكومية والقطاع الخاص والمؤسسات الخاصة والأفراد نتيجة لوباء (COVID-19)'' واعتماد ''التعليم الالكتروني'' مع انتشار أنظمة التعليم على الإنترنت بسرعة، تحذر اليونيسف من أن الأطفال معرضون لخطر متزايد، ''عرضة للاستغلال الجنسي عبر الإنترنت والاستمالة، حيث يتطلع المحتالون إلى استغلال جائحة (COVID-19)، حيث هنالك وجه آخر يتعلق بالنشاط الإجرامي الذي يستهدف أموال الإغاثة التي زادتهاالحكومات لمساعدة مواطنيها الذين يكافحون مالياً خلال هذه الأزمة''.

قدّر مايكل دامبروسيو (Ambrosio'MichaelD)[27]، مساعد مدير مكتب التحقيقات في الخدمة السرية، الخسائر المحتملة من حزمة التحفيز (Act CARES) البالغة قيمتها 3 تريليونات دولار، يمكن أن تصل إلى (30) مليار دولار، إذا افترضنا معدل احتيال منخفض للغاية، بنسبة (1%) فقط، يتمثل جانب مختلف من نشاط المجرمين السيبرانيين المرتبط بـ (COVID-19) في زيادة استهداف المرافق الطبية والبحثية، أدى الهجوم السيبراني على مستشفى جامعة برنو في جمهورية التشيك في منتصف شهر اذار إلى بلورة العديد من المخاوف المتعلقة بالأمنللمرافق الطبية والبحثية وتسليط الضوء على الوباء، وبحسب ما ورد اضطر المستشفى إلى إغلاق شبكة تكنولوجيا المعلومات الخاصة به، وتأجيل العمليات الجراحية واضطراره إلى إعادة توجيه المرضى إلى مستشفيات أخرى.

27-ايكل دمبروسي: هو مساعد مدير مكتب التحقيقات: في منصبه الحالي، السيد D›Ambrosio هو المدير التنفيذي الأول الذي يقود 162 مكتبًا ميدانيًا للخدمة السرية، والتي تحارب الجرائم الإلكترونية وتحمي النظام المالي الأمريكي، بالإضافة إلى ذلك، فإن السيد دامبروسيو مسؤول عن إدارة وتوفير الموارد لـ 40 فرقة عمل معنية بالجرائم الإلكترونية (ECTF) و 46 فريق عمل خاص بالجرائم المالية (FCTF)، بدأ السيد D›Ambrosio حياته المهنية في الخدمة السرية في عام 1997، كوكيل خاص تم تعيينه في مكتب نيويورك الميداني، بعد أن خدم لمدة 5 سنوات كضابط مشاة في سلاح مشاة البحرية الأمريكية. حصل على بكالوريوس إدارة الأعمال من كلية سيينا، ألباني، نيويورك، ودرجة الماجستير في العلوم في استراتيجية الأمن القومي من الكلية الحربية الوطنية، وماجستير العلوم في العدالة الجنائية من جامعة سينسيناتي:

/https://www. cybercon. us/speakers/michael-dambrosio

بعد فترة وجيزة، أصدر الإنتربول إشعاراً أرجوانياً يحذر من ''زيادة كبيرة في عدد محاولات هجمات الفدية ضد المؤسسات الرئيسة والبنية التحتية المشاركة في الاستجابة للفيروس''، أبلغ مكتب التحقيقات الفيدرالي و(CISA) أن الجهات الفاعلة التابعة للصين استهدفت المنظمات الأمريكية، ''في محاولة لتحديد الملكية الفكرية (IP) وبيانات الصحة العامة المتعلقة باللقاحات والعلاجات والاختبار من الشبكات والأفراد المرتبطين بـ (COVID-19) والحصول عليها بشكل غير المشروع، '' صرح رئيس المفوضية الأوروبية علناً أن الصين ''ربما كانت'' وراء عدد من الهجمات السيبرانية ضد المستشفيات الأوروبية وأن مثل هذا الإجراء ''لا يمكن التسامح معه.

الملحق ب: أكثر أنواع الجرائم السيبرانية تكلفة

البرامج الضارة وبرامج التجسس

استناداً إلى بيانات الاستطلاع، فإن برامج التجسس والبرامج الضارة (بما في ذلك الفيروسات والديدان وبرامج التجسس وkeyloggers وأحصنة طروادة) كلفت المؤسسات الكثير في العام 2019، تسهل البرامج الضارة مجموعة من الأنشطة الإجرامية، من برامج الفدية وتسلل البيانات إلى التعطيل النشط للشبكات، تعد التعاملات غير المشروعة مع الجرائم السيبرانية كخدمة للبرامج الضارة بأن تصبح أكثر تقدماً في الوقت نفسه وأكثر سهولة في الوصول إليها لمن ليس لديهم خبرة تقنية عميقة، كما أن أسواق الجريمة السيبرانية، قد شهدتظهور بائعين متخصصين ليسوا خبراء في تصميم البرامج الضارة فحسب، بل أيضاً في إنشاء البنية التحتية اللازمة للهجوم، حيث يعرضون تأجير البرامج الضارة لمجرمي الإنترنت المحتملين مقابل رسوم، ما يخلق بيئة يمكن لمجموعة صغيرة من المجرمين ذوي التفكير التقني تركيز اهتمامهم الكامل على تطوير قدرات هجوم جديدة، وحيث يمكن لمجموعة كبيرة من الجهات الفاعلة الأقل تطوراً الاستفادة منها بسهولة.

خروقات البيانات

في النصف الأول من عام 2019، تم الإبلاغ عن أكثر من (3800) انتهاك للبيانات، ما أدى إلى تعريض أكثر من أربعة مليارات سجل لمجرمي الإنترنت، واحدة من المجموعات الفرعية المتعلقة بانتهاكات البيانات هي تلك التي تؤثر على البيانات الصحية الشخصية، يمكن أن تكون هذه البيانات غالباً واحدة من أكثر أشكال البيانات قيمة للمجرمين نظراً للطريقة التي تتيح بها الاستهداف الدقيق للمخططات الاحتيالية للأفراد المعرضين للخطر بناءً على تاريخهم الطبي، ابتداءً

من آب 2020، كانت وزارة الصحة والخدمات الإنسانية الأمريكية تحقق في أكثر من (550) حالة من حالات انتهاك المعلومات الصحية الشخصية الناجمة عن السرقة أو القرصنة أو حوادث تكنولوجيا المعلومات أو الوصول غير المصرح به، تشمل هذه الحالات بيانات ما يقرب من (35) مليون فرد.

غالباً ما تكون خروقات البيانات نتيجة لجهات فاعلة خارجية، ولكن وجدت دراسة حديثة أن العديد منها ناتج عن هجمات من الداخل ومن الأمثلة على ذلك حالة شركة(28)(Tesla) في عام 2018، عندما أساء موظف استخدام وصوله لإجراء تغييرات "ضارة" على شفرة المصدر لنظام التشغيل التصنيعي للشركة)، وقام بنقل وحدات غيغابايت من المعلومات حول عمليات التصنيع في Tesla إلى طرف ثالث.

التصيد

وفقاً لمجموعة عمل مكافحة التصيد (APWG)(29)، تم تسجيل أكثر من(165000) موقع فريد للتصيد الاحتيالي في الربع الأول من عام 2020. أصبح التصيد الاحتيالي أسهل في السنوات الأخيرة، حيث ظهرت عروض التصيد كخدمة في أسواق الجرائم السيبرانية، بفضل هذه

28- تسلا (Tesla، Inc): هي شركة تقع في كاليفورنيا متخصصة في صناعة السيارات الكهربائية، والمكونات الكهربائيّة للقطارات الكهربائية. هي شركة عامة يتم تداول أسهمها في بورصة ناسداك بشعار TESLA، وقد حازت أرباحًا بعدَ 10 سنواتٍ في الربع الأول عام 2013، يُعتبر ما جذب انتباهاً واسعاً لشركة تسلا هو إنتاجها لسيارات كهربائية من نوع سيدان، وعملية مثل السيارة تسلا طراز إس. تقوم الشركة أيضاً ببيع مجموعات بطاريات الليثيوم أيون لشركات عالمية، لاستخدامها في القطارات الكهربائية، وقد أعلن مجلس إدارة الشركة أنه يسعى للإنتاج الكمي للسيّارات الكهربائية، لخفض تكلفتها لتكون في متناول المستهلك المتوسط، في 1 يوليو 2020، وصلت تسلا إلى القيمة السوقية 206. 5 بليون دولار، متجاوزة تويوتا، وأصبحت بذلك شركة السيَّارات الأكثر قيمة بالعالم، كانت تسلا موضوعاً للعديد من الدعاوى القضائية والخلافات، الناشئة عن تصريحات وسلوك الرئيس التنفيذيّ إيلون ماسك، ومزاعم انتقام المبلغين عن المخالفات، وانتهاكات حقوق العمّال المزعومة، والمشاكل التقنيَّة والخطيرة معَ منتجاتها التي لم يتم حلها، تُعدّ تسلا أيضًا واحدة من أكثر الشركات للبيع المكشوف في التاريخ: https://ar. wikipedia. org/wiki

29-مجموعة عمل مكافحة التصيد الاحتيالي (APWG) :عبارة عن اتحاد دولي يجمع بين الشركات المتضررة من هجمات التصيد، وشركات المنتجات والخدمات الأمنية، ووكالات إنفاذ القانون، والوكالات الحكومية، والجمعيات التجارية، ومنظمات المعاهدات الدولية الإقليمية، وشركات الاتصالات، تأسست في عام 2003 من قبل David Jevans، تضم APWG أكثر من 3200 عضو من أكثر من 1700 شركة ووكالة في جميع أنحاء العالم، تشمل الشركات الأعضاء شركات أمنية رائدة مثل Kaspersky Lab و BitDefender و Symantec و McAfee و VeriSign و IronKey و Internet Identity. يشمل أعضاء الصناعة المالية مجموعة ING و VISA و MasterCard و American Bankers Association. https://en. wikipedia. org/wiki/Anti-Phishing_Working_Group

العروض، لم يعد مجرمو الإنترنت بحاجة إلى خبرة في تصميم البنية التحتية للتصيد الاحتيالي، بدلاً من ذلك، يمكن للمجرمين ببساطة الشراء من البائعين الذين يعؤضون مجموعاتهم الخاصة والتركيز على الضحايا (الذين تتوفر أيضاً تفاصيل الاتصال بهم بسهولة من نفس الأسواق)، وجدت إحدى المجموعات البحثية أكثر من (5000) مجموعة من مجموعات التصيد الاحتيالي الجاهزة للاستخدام في النصف الأول من عام 2019 وحده.

برامج الفدية

تظل برامج الفدية الجزء الأسرع نمواً في الجرائم السيبرانية، خلال جائحة(COVID-19)، زادت هجمات برامج الفدية بشكل عام بنسبة (148 %) عن مستويات خط الأساس التي تم الإبلاغ عنها في شباط 2020.

أحد أكثر الاتجاهات إثارة للقلق في برامج الفدية هو التحول نحو الأهداف في الصناعة التحويلية، بدأ باحثوا الأمن في رؤية ظهور سلالات برامج الفدية التي تستهدف أنظمة التحكم الصناعية، وقد دفع ضحايا الصناعة بالفعل ملايين الدولارات كفدية للذين وقعوا فريسة لهذه المتغيرات، من المحتمل أن يستمر هذا الاتجاه إذ تستعد المصانع ومشغلي الصناعة الآخرين لتوسيع نشرهم لأجهزة إنترنت الأشياء المعرضة للخطر في جميع أماكن عملهم، مما يؤدي إلى توسيع سطح الهجوم لشبكتهم وإنشاء أهداف جديدة للجهات الفاعلة الخبيثة.

كما تعرضت المؤسسات المالية للهجوم من قبل الدول، في عام 2016، تمكن قراصنة كوريون شماليون من سرقة (81) مليون دولار من البنك المركزي البنغلاديشي من خلال الاستفادة من أوراق الاعتماد المسروقة وتقديم طلبات تحويل أموال مزيفة إلى بنك الاحتياطي الفيدرالي في نيويورك، في الآونة الأخيرة، في عام 2018، تمكنت نفس المجموعة من المتسللين من سرقة 20 مليون دولار من بنك (Bancomext) المكسيكي، ويمكن رؤية حجم التهديد الذي يواجه المؤسسات المالية بشكل أكثر وضوحاً حين نعلم أنه خلال لقاء القبض على زعيم عصابة جرائم سيبرانية عام 2018 تبينقيام مجموعته بسرقة (1. 2) مليار دولار من أكثر من 100 بنك على مدى خمس سنوات.

اختراق البريد الإلكتروني للأعمال

على الرغم من أن البنوك لا تزال هدفاً مفضلاً لمجرمي الإنترنت، فقد حدثت أيضاً زيادة في استخدام العمليات الاحتيالية (BEC)(30)، وهي فئة خاصة من سرقة الهوية، عادةً ما تستهدف هذه المخططات قسم الموارد البشرية في الشركة أو قسم الرواتب من خلال التظاهر كموظف يطلب تغيير معلومات الإيداع المباشر الخاصة به، بعد ذلك، يتم تحويل شيك راتب الموظف إلى حساب بطاقة مسبقة الدفع احتيالي، تتضمن الأشكال الأخرى من عمليات الاحتيال ((BEC حسابات البريد الإلكتروني للموردين والمحامين المخادعين وطلبات أنموذج (W-2) والطلبات الاحتيالية لبطاقات الهدايا، يسمح هذا لمجرمي الإنترنت بإرسال رسائل بريد إلكتروني تنتحل صفة أي موظف – من الموظفين الجدد إلى المدير التنفيذي.

بشكل عام، تمثل عمليات الاحتيال (BEC) تحديات خاصة للبنوك، حيث قد يبدو أن طلب التحويل البنكي قد تم تقديمه من قبل عميل شرعي، ومع ذلك، قد يتم استغلال بيانات اعتماد هذا الشخص بواسطة مجرمي الإنترنت لأغراض شائنة.

في أيار 2020، أفادت شركة (Virtual Financial)، إحدى الشركات العالمية الرائدة في مجال الخدمات المالية وصنع السوق، أنها وقعت ضحية لعملية احتيال بقيمة(6. 9) مليون دولار أمريكي، أرسل المتسللون عدة رسائل بريد إلكتروني تنتحل شخصية الرئيس التنفيذي إلى قسم المحاسبة، اعتقاداً بأن الطلبات مشروعة، امتثل قسم المحاسبة في (Virtu) للطلبات، بعد أن أرسل قسم المحاسبة الأموال، قام قسم التدقيق الداخلي في (Virtu) بوضع علامة على التحويلات على أنها احتيالية.

30- (BEC): يستخدم النشاط التجاري العادي البريد الإلكتروني لكل شيء بدءاً من دعم العملاء وحتى الموارد البشرية، ويترتب على ذلك أنه عندما تستهدف إحدى الهجمات السيبرانية شركة ما، فإن البريد الإلكتروني هو مكان منطقي لبدء هذه الهجمات، أحد الأمثلة على ذلك هو عملية احتيال البريد الإلكتروني الخاصة بالعمل (BEC)، تستخدم عملية احتيال BEC مزيجاً من الهندسة الاجتماعية والتوجيه الخاطئ لتشجيع الموظفين على البدء في إرسال التحويلات البرقية إلى الغرباء، وبطبيعة الحال، فهي أيضاً واحدة من أغلى عمليات الاحتيال التي يمكن أن تقع الأعمال ضحية لها، إذن ما هي عملية احتيال BEC بالضبط، وكيف تعمل؟ كيف يمكنك تجنب الوقوع ضحية لأحد؟عملية احتيال BEC هي عندما يستخدم المهاجم بريداً إلكترونياً لانتحال شخصية شخص آخر في محاولة لاستخراج تحويل إلكتروني أو مورد آخر من شركة، يُعرف أيضاً باسم احتيال الرجل في البريد الإلكتروني، تشبه عمليات الاحتيال BEC هجمات Man-in-the-middle من حيث أنها تعتمد على اعتقاد الضحية أنهم يتواصلون مع شخص آخر، تعتبر عمليات احتيال BEC فعالة لأن الضحية عادة ما تكون له علاقة سابقة بالشخص الذي يتم انتحال هويته، وهذه مشكلة واسعة الانتشار، أفاد مكتب التحقيقات الفيدرالي (FBI) أن عمليات الاحتيال BEC كلفت الشركات الأمريكية (1، 8) مليار دولار في العام 2020 وحده:https://tiknulujia. istocks. club/2021-05-25/

سرقة العملات المشفرة

لا تزال سرقة العملات المشفرة تمثل اتجاهاً رئيساً في الجرائم السيبرانية، إذ سُرقت أكثر من 4 مليارات دولار من العملات المشفرة على مدار عام 2019 وحوالي (1، 4) مليار دولار سُرقت في الأشهر الخمسة الأولى من عام 2020، تحدث هذه السرقات غالباً من عمليات التبادل والمحافظ التي يحتفظ بها مستخدمون عملاتهم المعدنية، باستخدام مجموعة من التكتيكات بما في ذلك التصيد والبرامج الضارة والسرقة من الداخل، هنالك اتجاه ناشئ آخر وهو(التعدين) Cryptojacking)) (31)، إذ يتم تثبيت البرامج الضارة على أجهزة كمبيوتر الضحايا لتعدين العملات المشفرة عن بُعد، قد لا يلاحظ المستخدمون وقت حدوث عمليات الـ (Cryptojacking)، ولكن يمكن أن يؤدي ذلك إلى إبطاء الأجهزة المتأثرة وسحب تكاليف الكهرباء أثناء حدوث التعدين.

أصبحت مخططات الجرائم السيبرانية المدعومة بالذكاء الاصطناعي التي تستخدم الوسائط المصنّعة أكثر انتشاراً، لا تشمل الوسائط الاصطناعية محتوى الصور والفيديو "المزيف العميق" فحسب، بل تشمل أيضاً الصوت المزيف والوسائط المكتوبة، مثل أتمتة معلومات التهديدات باستخدام التعلم الآلي، لا يزال خبراء الصناعة قلقين بشأن الاستخدامات الهجومية للذكاء الاصطناعي في الجرائم السيبرانية، يفترض بعض الخبراء أن التزييف العميق يمكن أن يصبح مصدراً خبيثاً للاستغلال وللمعلومات المضللة والمواد الإباحية غير الرضائية، مع اكتساب تقنية مبادلة الوجه مزيداً من الشعبية، يثير بعض الخبراء مخاوف من احتمال استخدام هذه التكنولوجيا أيضاً بواسطة المجرمين لغايات خبيثة مثل الابتزاز والاحتيال الرومانسي وغير ذلك.

الملحق ج: من هم المجرمون؟

أصبحت الجرائم السيبرانية الآن نشاطاً "احترافياً" متخصصاً، لا يزال هنالك العديد من الوافدين الجدد غير المتمرسين، ولكن إذا كانوا يعيشون في بلدان حيث سيادة القانون قوية، فعادة ما ينتهي بهم الأمر في السجن، يزدهر مجرمو الإنترنت عندما يكون تطبيق القانون ضعيفاً، سواء

31- Cryptojackin: هو الاستخدام غير المصرح به لجهاز كمبيوتر شخص آخر لتعدين العملة المشفرة، يقوم المتسللون بذلك إما عن طريق جعل الضحية تنقر على رابط ضار في رسالة بريد إلكتروني تقوم بتحميل رمز تشفير على الكمبيوتر، أو عن طريق إصابة موقع ويب أو إعلان عبر الإنترنت بشفرة JavaScript)) يتم تنفيذها تلقائياً بمجرد تحميلها في متصفح الضحية.

https://www. csoonline. com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it. html

كان ذلك بسبب عدم تطوير العديد من البلدان للقدرات اللازمة لمكافحة الجريمة السيبرانية أو لأن حكومتها قررت غض الطرف عن هذا النوع من الأنشطة الجرمية.

يعني الانتشار العالمي للإنترنت أن المجرمين والضحايا لا يحتاجون إلى أن يكونوا موجودين في نفس المكان، كما أوضح مدير مكتب التحقيقات الفدرالي الامريكي (كريستوفر وراي) في القمة الوطنية للأمن السيبراني في العام 2020، ''علينا تغيير حساب التكلفة والعائد للمجرمين والدول القومية التي تعتقد أنها يمكن أن تعرض شبكات الولايات المتحدة الامريكية للخطروسرقة الملكية الفكرية والمالية الأمريكيةوجعل البنية التحتية الحيوية في خطر، كل ذلك دون تتحمل أي مخاطر، بالنسبة لمعظم البلدان، ستُعزى الغالبية العظمى من خسائر الجرائم السيبرانية إلى جهات فاعلة خارج نطاق ولايتها القضائية، أصبحت الجرائم السيبرانية من بين الأنشطة الأكثر ربحاً، مع تداول البيانات وبرامج الفدية، بالنسبة لمعظم البلدان، ، حيث أصبح تداول البيانات وبرامج الفدية أدوات شائعة بشكل متزايد، منذ كانون الثاني إلى حزيران من عام 2020، تكبدابرزضحايا 11 هجوماً لبرامج الفدية في أوروبا والولايات المتحدة الامريكية، في كل من القطاعين الخاص والعام، خسائر مالية قدرها (144. 2) مليون دولار مرتبطة بإعادة بناء البنية التحتية ودفع الفدية وإنشاء برامج جديدة.

بالنسبة للهياكل الأمنية، تتمتع فرق مكافحة الجرائم السيبرانية المنظمة بدرجة عالية من التنظيم، مع قادة الفرق والمبرمجين ومسؤولي الشبكات والمتخصصين في التسلل ومنقبين البيانات وحتى المتخصصين الماليين الذين يقودون مؤسسات ضخمة من المتسللين متعددي الجنسيات، في الآونة الأخيرة، بدأت بعض المجموعات التي لم تكن مترابطة سابقاً في التعاون مع بعضها البعض من أجل زيادة أنشطتها وأرباحها، في الصين وحدها، يعمل ما يقدر بنحو (400) ألف شخص في شبكات جرائم الإنترنت المنظمة سريعة النمو، بعض البلدان هي بؤر للجرائم السيبرانية، إن ضعف سيادة القانون، والافتقار إلى وكلاء إنفاذ القانون المتخصصين، والموارد غير الكافية تسمح لمجرمي الإنترنت بالإثراء مع الإفلات من العقاب، في نيجيريا على سبيل المثال، تساعد البطالة وسوء تنفيذ القوانين ووكالات إنفاذ القانون غير المجهزة بشكل كافٍ في تفسير سبب ازدهار الجريمة السيبرانية، لسنوات؛ أدى النمو الاقتصادي السريع وعدم القدرة على استيعاب المواهب إلى اعتبار فيتنام ''مركزاً متوسط المستوى للجرائم السيبرانية''.

ومع ذلك، تتمتع الدول الأخرى ببيئة متساهلة لمجرمي الإنترنت وتستخدمها لأغراض الدولة

عند الحاجة، في روسيا على سبيل المثال، فإن العلاقة المعقدة والوثيقة بين الدولة والجريمة المنظمة تجعلها ملاذاً لمجرمي الإنترنت الأكثر تقدماً، والسماح للجماعات الإجرامية بمتابعة مخططاتها ذات الدوافع المالية وحمايتها من إنفاذ القانون له ثمن، إذ من المتوقع أن يستخدموا مهاراتهم لدعم مصالح الحكومة، قال (جون كارلين) مساعد المدعي العام السابق لقسم الأمن القومي بوزارة العدل الأمريكية، ''بشكل متزايد، لا يمكنك معرفة أيهما(المجرمين ام الدولة) عندما يتعلق الأمر بالجريمة ووكالة الاستخبارات، لذلك، في يوم من الأيام، قد يفعل المحتال نفسه شيئاً لمجرد كسب المال، لكن هذا المحتال نفسه قد يتم توجيهه بواسطة عميل استخبارات مدرب باستخدام نفس الأدوات والأساليب لسرقة المعلومات من أجل أهداف الدولة''.

عند إصدار عقوبات ضد (مكسيم ياكوبيتس)، زعيم مجموعة الجرائم السيبرانية (Evil Corp)، أوضح المسؤولون الأمريكيون ''مسؤوليته المباشرة في دعم الجهود السيبرانية الخبيثة للحكومة الروسية''، بالإضافة إلى جرائمه ذات الدوافع المالية، يبدو أن هذه العلاقة التكافلية هي أيضاً الحالة في إيران، حيث يتصرف مجرمو الإنترنت، في كثير من الحالات، لتحقيق مكاسب خاصة و مكاسب لصالح الحكومة، وجدت التهم الأخيرة ضد اثنين من المتسللين الإيرانيين أنه في نفس ''حملة السرقة السيبرانية''، كانت هنالك حالات تصرفوا فيها ''بأمر من إيران''، وأحياناً لتحقيق مكاسب مالية فقط، قراصنة (معهد مابنا) سرقوا أبحاثاً من جامعات وحكومات و الشركات في جميع أنحاء العالم، والتي كلفت المؤسسات أكثر من 3 مليارات دولار.

وقد انخرطت بعض الدول بشكل مباشر في جرائم الإنترنت لتحقيق مكاسب مالية خاصة بها، تستخدم كوريا الشمالية عمليات السرقة وغسيل الأموال عبر الإنترنت وحملات الابتزاز والتشفير لتمويل مشاريعها، قد تكون كوريا الشمالية قد قامت بتحويل ما يصل إلى 2 مليار دولار من الجرائم السيبرانية ضد البنوك وعمليات تبادل العملات المشفرة إلى أبحاث أسلحة الدمار الشامل (WMD)، ''لتوليد الدخل بطرق يصعب تتبعها'' مثل اختراقان عام 2019 سرقة 250 مليون دولار من العملات المشفرة.

(برنامج الفدية) هي أداة أخرى مفضلة، من خلال جعل الفدية أرخص من تكلفة النسخ الاحتياطي والاستعادة، فإنهم يسعون إلى إجبار الشركات على الدفع، لقد ناقشنا كيف يمكن لسرقة بروتوكول الإنترنت، كتكلفة خفية، أن تمثل خسارة كبيرة للوكالات والشركات، فضلاً عن كونها تشكل خطراً على الأمن القومي، يصعب محاربة هذا النوع من الجرائم عندما تكون مدعومة

من الدولة، لطالما كان التجسس الاقتصادي لصالح الصناعة الوطنية سمة مميزة لسياسة الصين الاقتصادية، تمثل الصين ما يقرب من(80 %) من جميع حالات التجسس الاقتصادي في الولايات المتحدة الامريكية، وقد كلفت الاقتصاد الأمريكي حوالي ''نصف تريليون إلى تريليون دولار من الأضرار''. تلعب السرقة السيبرانية دوراً مهماً في جعل هذا الأمر ناجحاً سياسياً، تشمل الأهداف الانموذجية للمتسللين الصينيين المرتبطين بالدولة شركات الدفاع والتكنولوجيا والشركات الهندسية ومطوري الأجهزة الصيدلانية والطبية.

وسط جائحة (COVID-19)، ازداد استهداف مرافق الرعاية الصحية والبحوث الطبية، اقترح رئيس مفوضية الاتحاد الأوروبي أن الصين قد تكون وراء هذه العمليات وأشار إلى أن هذا لن ''يتم التسامح معه''، في حدث ذي صلة، أصدرت وزارة العدل الأمريكية لائحة اتهام في تموز الماضي ضد اثنين من المتسللين الصينيين يستهدفون (IP)، بما في ذلك ابحاث ((COVID-19 تزعم الوثيقة أنهم في بعض الأحيان ''تصرفوا لتحقيق مكاسب مالية شخصية خاصة بهم''، وفي بعض الحالات، تصرفوا لصالح وكالات حكومية، المتسللين الذين يتم القبض عليهم بواسطة الشرطة الصينية يُعرض عليهم الاختيار: العمل لصالح الدولة أو الذهاب إلى السجن.

الملحق د: الخبرات الوطنية

وجد الاستطلاع الذي أجريناه أن المؤسسات في البلدان المختلفة تقيم المخاطر السيبرانية بشكل مختلف، في حين أن العديد من النتائج صحيحة في جميع أنحاء العالم، فإن بعض القيم المتطرفة تساعدنا في وضع خطط أفضل لزيادة الكفاءة، لا يوجد حل مقاس واحد يناسب الجميع فيما يتعلق بالمخاطر السيبرانية، على الرغم من أن النتائج التي توصلنا إليها محدودة بالمواقع التي تم مسحها (الولايات المتحدة وكندا والمملكة المتحدة وفرنسا وألمانيا وأستراليا واليابان)، فإنها توفر لقطات مفيدة من الاختلافات عبر البلدان.

أجرت المؤسسات 18 تحقيقاً في مجال أمن تكنولوجيا المعلومات في المتوسط في عام 2019. وأجرت المؤسسات الألمانية والأمريكية والبريطانية تحقيقات فوق المتوسط، مع وجود مؤسسةفرنسية في الطرف الأدنى من الطيف، قد يشير هذا إلى أن المؤسسات في فرنسا تواجه مخاطر أقل أو أنها لا تولي اهتماما لها، أفادت (32%) من المؤسسات الفرنسية أنها لم تتعرض لحادث سيبراني تسبب في توقف العمل، بينما كان ذلك صحيحاً فقط لمتوسط (26%) من إجمالي المستجيبين.

نظراً لكون وقت التوقف عن العمل نتيجة شائعة لحوالي ثلثي مؤسسات المستجيبين، يبدو أن الموقع يُحدث فرقاً. (40%) من الشركات أو الوكالات في اليابان لم تشهد أي توقف، بينما كان هذا صحيحًا فقط لـ (18%) منهم في الولايات المتحدة الامريكية –يمكن تفسير ذلك إذا نفذت المؤسسات اليابانية تدابير وقائية أفضل– لكن لا يبدو أنها تفعل شيئاً مختلفاً عن الآخرين في الولايات المتحدة، تطوير خطط الوقاية والاستجابة، تفسير آخر معقول هو أن المؤسسات في الولايات المتحدةالامريكية هي أهداف أكثر إغراءً وربحاً، على الرغم من أنه في بعض الحالات بدا أن هنالك صلة بين مدة التوقف والتكاليف المرتبطة بها، إلا أن هذا لم يكن صحيحاً دائماً، كان متوسط تكلفة أطول فترة توقف للمؤسسات في كل من اليابان وألمانيا أعلى من مليون دولار، وعلى الرغم من أن مدة التوقف في اليابان كانت أعلى قليلاً من المتوسط عند 19 ساعة، كانت ألمانيا في النطاق الأدنى عند 14 ساعة الاستجابة للحادث.

استغرق الأمر 19 ساعة في المتوسط لمعظم المؤسسات للانتقال من اكتشاف حادثة إلى علاجها، يستلزم هذا عادةً استعادة خدمات تكنولوجيا المعلومات إلى السعة الطبيعية، وإزالة التهديد من النظام، واستعادة البيانات المفقودة، ومع ذلك، في بعض الحالات، لن تنظر المؤسسات في معالجة الحادث حتى يتم تحديد مصدر الحادث أو يتم تنفيذ بعض التدابير لمنع وقوع الحادث في المستقبل.

خلال أطول حادث يتعلق بأمن تكنولوجيا المعلومات، انقضت 15 ساعة قبل اكتشاف الاختراق، كان وقت الضعف الشديد هذا أطول بالنسبة للمؤسسات في اليابان والولايات المتحدةالامريكية وكندا، في حالة اليابان، استغرقت الشركات والوكالات وقتاً أطول بكثير من نظيراتها في البلدان الأخرى للانتقال إلى العلاج، واستغرق الأمر 48 ساعة، أي 20 ساعة أطول من المتوسط الإجمالي.

خطط الوقاية والاستجابة

لقد ناقشنا كيف أن الافتقار إلى خطط لمنع حوادث أمن تكنولوجيا المعلومات والاستجابة لها منتشر على نطاق واسع، حيث صرح (44%) فقط من المشاركين في الاستطلاع أن مؤسساتهم لديها كلاهما، وسجلت المؤسسات الفرنسية درجات أقل من ذلك، حيث تفتخر (26%) فقط من المؤسسات بخطط الوقاية والاستجابة، من غير المألوف أن لا يكون لدى المؤسسة أي نوع من

الخطط الموضوعة، حتى لو لم يكن لديهم خطط للوقاية والاستجابة، فسيكون لديهم واحد منها في مكانها، فقط في اليابان وجدنا نسبة أكبر من المؤسسات التي ليس لديها أي نوع من الخطط: (4% مقابل 1%) في المتوسط.

تعد المشاركة المحدودة لـ (C-suite)[32] في تطوير الخطط تجربة مشتركة عبر البلدان، ومع ذلك، من المثير للاهتمام ملاحظة من قرروا الشراكة، بينما تذهب الولايات المتحدة الامريكية وكندا والمملكة المتحدة البريطانية إلى إشراك الرئيس التنفيذي أو مجلس الإدارة، تميل مؤسسات في فرنسا وألمانيا إلى جلب CIO) و CISO و CTO) إلى حد أكبر.

استراتيجيات الاتصال

كانت الوكالات والشركات في كندا وألمانيا أقل احتمالية لمشاركة المعلومات حول أكثر حوادث أمن تكنولوجيا المعلومات خطورة مع أي شخص خارج مؤسساتهم، يمكن للمرء أن يفترض أن زيادة التقارير الإعلامية ستكون حافزاً للمؤسات للمضي قدماً في القصة وإعلام الجمهور، ومع ذلك، هذا ليس هو الحال، على الرغم من أن الحوادث التي تحدث في الولايات المتحدة الامريكية تحظى بأكبر قدر من اهتمام وسائل الإعلام – ردت (24%) من المؤسساتان أكثر حوادث أمن تكنولوجيا المعلومات خطورة قد تمت تغطيتها من قبل وسائل الإعلام (وهذا صحيح بالنسبة لمتوسط (16%) من إجمالي المؤسسات التي شملتها الدراسة) –(22%) من الشركات والوكالات الأمريكية التي تمت مقابلتها أفادت بأنها لم تشارك أي معلومات، لا يبدو أن التواصل مع العملاء يمثل أولوية في معظم البلدان، مع عدم وجود اختلافات كبيرة بين الأشخاص الذين تمت مقابلتهم: أبلغت (345) شركة فقط من أصل (1332) شركة عملائها بأنها تعرضت لحادث سيبراني.

32- C-suite، أو C-level، هي لغة عامية مستخدمة على نطاق واسع تصف مجموعة من كبار المديرين التنفيذيين في الشركة. يحصل C-suite على اسمه من ألقاب كبار المديرين التنفيذيين، والتي تميل إلى البدء بالحرف C، لـ «CEO»، كما هو الحال في الرئيس التنفيذي (CEO)، والمدير المالي (CFO)، ورئيس العمليات (COO)، ورئيس قسم المعلومات (CIO). https://www. investopedia. com/terms/c/c-suite. asp

الملحق هـ: دراسة حالة – جامعة ديوك

للمساعدة في تحديد شبكات الجامعة والدفاع عنها من المهاجمين، طور مكتب تكنولوجيا المعلومات بجامعة ديوك برنامج ذكاء التهديدات المشتركة لحراسة بوابة الشبكة والاستجابة الآلية من خلال برنامج (STINGAR) للتعليم العالي، يقوم ستينجار بتوفير معلومات استخباراتية عن التهديدات محلياً باستخدام شبكات الجذب المجتمعية عبر مؤسسات التعليم العالي الشريكة وهي مصممة لمواجهة التهديدات في الوقت الفعلي تقريباً، على سبيل المثال، في ذروة هجوم (botnet Mirai)[33] الشهير، ساعدت (STINGAR فريق Duke) الأمني في منع ما معدلهمليارين محاولة اتصال ضارة يومياً.

بمجرد أن بدأت جائحة (COVID-19) في التأثير على التعليم العالي، لاحظ مشروع STINGAR)) انخفاضاً أولياً في عناوين (IP) الخبيثة الفريدة (اذار ونيسان 2020)، حيث انتقل أعضاء هيئة التدريس والطلاب والموظفون إلى التعلم عن بُعد أو وضع العمل، يستخدم نظام (STINGAR) البيئي مستشعرات الشبكة (مواضع الجذب أو أجهزة الاستشعار الأخرى) لاكتشاف التهديدات المحتملة، وتمكين اتحاد بيانات التهديدات متعددة الجامعات، واستخدام مشغلات الشبكة لمنع التهديدات بسرعة في الوقت الفعلي القريب، في حين أن عدد عناوين(IP) الضارة الفريدة التي تم اكتشافها قد انتعش، إلا أن العدد الإجمالي للهجمات التي اكتشفتها (STINGAR) لا يزال بشكل عام أقل من المستويات التي كنا نشهدها قبل انتشار الوباء، ان هذا الانخفاض قد حدث نتيجة لسببين:

(أ) انخفاض الأنظمة على الشبكات المشاركة (بمجرد انتقال أعضاء هيئة التدريس والموظفين والطلاب إلى سيناريو التعلم / العمل عن بُعد، كان هناك نشاط محلي أقل).

33- Mirai botnet:هو برنامج ضار يحول الأجهزة المتصلة بالشبكة التي تعمل بنظام Linux إلى روبوتات يتم التحكم فيها عن بُعد والتي يمكن استخدامها كجزء من الروبوتات في هجمات الشبكة واسعة النطاق، يستهدف بشكل أساسي الأجهزة الاستهلاكية عبر الإنترنت مثل كاميرات (IP) وأجهزة التوجيه المنزلية، تم العثور على Mirai botnet لأول مرة في اب 2016 بواسطة MalwareMustDie، وهي مجموعة بحثية عن البرمجيات الخبيثة ذات قبعة بيضاء، وقد تم **استخدامها في** بعض أكبر هجمات الحرمان الموزع للخدمة (DDoS) وأكثرها اضطرابًا، بما في ذلك الهجوم على 20 سبتمبر 2016 على موقع الويب الخاص بصحفي أمن الكمبيوتر براين كريبس، هجوم على مضيف الويب الفرنسي OVH، وهجوم داين الإلكتروني في أكتوبر 2016، وفقاً لسجل الدردشة بين Anna-senpai و Robert Coelho، تم تسمية Mirai على اسم مسلسل الأنمي التلفزيوني Mirai Nikki:https://en. wikipedia. org/wiki/Mirai_(malware 2011)

(ب) التحول في التكتيكات لاستهداف العاملين من المنزل والمتعلمين عبر التصيد الاحتيالي أو هجمات الهندسة الاجتماعية الأخرى.

-استهدف الصين وروسيا وكوريا الشمالية وإيران للمؤسسات الأكاديمية الأمريكية: مشروع ستينجار:

من بين هذه المجموعة من الجهات الحكومية، وفقاً لبرنامج (STINGAR s'Duke)، من شباط 2020 إلى تموز 2020، يبدو أن غالبية طلبات عناوين IP)) الضارة نشأت من البنية التحتية المستضافة في الصين بناءً على عناوين (IP) الجديدة والفريدة التي تم اكتشافها، أرقام النظام الذاتي الرائدة (ASN) ذات العلاقات التنظيمية مع الصين هي رقم 31 شارع جين رونغ، بمتوسط(920، 5) عنوان (IP) فريد، UNICOM CHINA[34]، الصين Backbone. يشير ASN إلى مجموعة بادئات توجيه IP)) التي يديرها مشغلوا الشبكات لكيان ما، شارع Rong-Jin مدرج أيضاً في قائمة) Spamhaus[35] لأفضل 10 شبكات بوت نت[36].

تُظهر بيانات STINGAR من جامعة Duke شبكات ASN التي تنشأ منها الهجمات، ما يوفر مصدراً للمعلومات حول "النظافة" النسبية للشبكات، بالنظر على وجه التحديد إلى الصين وإيران وروسيا، كشفت بيانات استخبارات التهديد ((STINGAR الخاصة بشركة Duke عن نشاط يومي متسق من هذه البلدان من خلال محاولات الاتصال الخبيثة (إجمالي الهجمات، وعناوين IP الفريدة، وعناوين IP الجديدة للهجوم) ومن المثير للاهتمام،

34-: CHINA UNICOM شركة الصين المتحدة لشبكات الاتصالات المحدودة أو تشاينا يونيكوم هي شركة مملوكة للدولة الصينية. تشاينا يونيكوم هي رابع أكبر مزود لخدمات الهاتف المحمول في العالم من خلال قاعدة المشتركين:.https://ar. wikipedia. org/wiki

35-Spamhaus: هي منظمة دولية، يقع مقرها في كل من أندورا وجنيف، وقد أسسها ستيف لينفورد في عام 1998 لتتبع مرسلي البريد الإلكتروني العشوائي والأنشطة المتعلقة بالبريد الإلكتروني العشوائي. صاغ Linford الاسم spamhaus، وهو تعبير ألماني زائف، للإشارة إلى مزود خدمة الإنترنت، أو شركة أخرى، والتي تقوم بإرسال بريد عشوائي أو تقدم خدمة عن عمد لمرسلي البريد العشوائي. https://en. wikipedia. org/wiki/The_Spamhaus_Project

36-البونت نت (BOTNET):هو مجموعةٌ من أجهزةٍ متصلةٍ ببعضها عبر شبكة إنترنت، قد تكون هذه الأجهزة حواسب أو هواتف ذكية أو خوادم أو أجهزة أخرى تعرف بإنترنت الأشياء، وجميع هذه الأجهزة المتصلة تكون مصابةً ويتم التحكم بها عبر نوع من البرامج الخبيثة، وفي حالاتٍ عديدةٍ قد لا يدرك المستخدم أن حاسبه يتعرض لهجومٍ أو إصابة بوت نت. الأجهزة المصابة يتم التحكم بها عبر منفذين للجرائم أو مفتعلي المشاكل، أحيانا ما يكونوا مجرمي إنترنت، ويتم استغلال الأجهزة المصابة أو الضحية لعملياتٍ معيّنةٍ ومحددةٍ، كي لا يلاحظ المستخدم شيء، وبالتالي تبقى العمليات الخبيثة مخفيةً عن عينه وإدراكه:https:// www. arageek. com/lAA-botnet

في وقت كتابة هذا التقرير، أنه لم يتم اكتشاف أي هجمات (IP) جديدة من كوريا الشمالية منذ نيسان 2020.

تحليل البيانات

روسيا:

1. متوسط إجمالي الاتصال اليومي هو (71، 916) اتصالاً، ومتوسط يومي فريد يبلغ (3، 491) اتصالاً.
2. انخفاض حاد في عدد الاتصالات اليومية في نهاية شهر اذار، حيث ظل رقم الاتصال اليومي أقل من المعتاد منذ الانتقال، يتوافق هذا مع توقيت انتقال معظم مؤسسات التعليم العالي إلى التعلم عن بعد والعمل.

الصين:

1. يبلغ متوسط إجمالي الاتصال اليومي (33. 292) اتصالاً، ومتوسط يومي فريد يبلغ (5. 108) بروتوكول إنترنت.
2. ظل النشاط الضار من عناوين (PI) الصينية ثابتاً إلى حد كبير خلال الأشهر الستة الماضية، كانت هنالك زيادة ملحوظة في عدد الاتصالات الإجمالية وعناوين PI)) الفريدة وعناوين (PI) الجديدة في 91 ايار و2 حزيران.

كوريا الشمالية:

1. متوسط إجمالي الاتصال اليومي يبلغ خمسة، ومتوسط PI الفريد اليومي (1).
2. تمت ملاحظة عدد قليل جداً من محاولات الاتصال الخبيثة من عناوين(PI) الخاصة بكوريا الشمالية في هذه الفترة.

إيران:

1. يبلغ متوسط إجمالي الاتصال اليومي (2، 656)، ومتوسط PI الفريد اليومي يبلغ (1، 812).
2. ظلت محاولات الاتصال الخبيثة من فضاء (PI) الإيراني متسقة على مدار العام، مع ارتفاع ملحوظ في أواخر أيار.