ملف اقتصادي

نشدد في حواره مع «الأنباء» على ضرورة تشريع قوانين خاصة للاختراقات المصرفية

الكندري: عقوبة الجرائم الإلكترونية والاختراقات غير المشروعة بالكويت تصل إلى 3 سنوات

عبدالله الكندري

المحامي عبدالله الكندري متحدثا للزميل محمود فاروق (سالم الشمري)

أكد المحامي عبدالله الكندري أن ظاهرة الجرائم الالكترونية على القطاعات الاقتصادية ظهرت في الآونة الأخيرة بعد التطور الحديث في مجال المعلومات والاتصالات وانتشار استخدام الحاسب الآلي، والمواقع الإلكترونية في شتى الأنشطة الاقتصادية.

وقال الكندري في حوار خاص لـ «الأنباء» ان الكويت بحاجة إلى تشريع قوانين خاصة تتعلق بالجرائم الالكترونية نظرا لان ما يطبق حاليا يدخل في اطار القوانين العامة، لافتا إلى ان عقوبة الجرائم الالكترونية وفقا للقوانين المعمول بها حاليا تصل إلى ثلاث سنوات فقط في حين ان هناك دولا عربية وأجنبية لديها قوانين خاصة لهذه النوعية من الجرائم وتصل عقوبتها إلى 10 سنوات.

واوضح الكندري ان تلك الجرائم المستحدثة علينا من شأنها الاعتداء على المعلومات الشخصية وعلى الأموال ايضا عبر الدخول غير المشروع على حسابات العملاء والمواقع المصرفية والاستيلاء على أموال أصحابها أو نقل معلومات سرية من هذه المواقع بدون إذن الامر الذي اثار ضجة خلال الآونة الاخيرة ما يدعو الى ضرورة التصدي لها وإيجاد رادع قانوني للخارجين على القانون خاصة بعد أن اثارت عدة تساؤلات قانونية عن التكييف القانوني لهذه الأفعال وما اذا كانت تشكل جناية أم جنحة ونصوص التجريم المطبقة عليها والمحكمة المختصة بنظرها وللإجابة عن تلك التساؤلات في الحوار التالي:

مجرمو المعلومات بالكويت مصنفون إلى مخترقين وحاقدين.. والمخترقون أكثرهم خطورة

التكييف القانوني لظاهرة الجرائم الإلكترونية مازال يشكل تساؤلاً ما إذا كانت تندرج تحت الجناية أم الجنحة

بداية هل لك ان تحدثنا عن الجرائم الالكترونية في الكويت من الناحية القانونية؟

● وفق آخر تعريف للجرائم الإلكترونية تم تصنيف مجرمي المعلومات إلى المخترقين والمحترفين والحاقدين.

أولا- المخترقون: مثل الهاكرز الذي يعتبر شخصا بارعا في استخدام الحاسب الآلي ولديه فضول في استخدام حسابات الآخرين بطرق غير مشروعة الأمر الذي يدل على أنهم أشخاص متطفلون وغير مرحب بهم لدى الغير، وأغلبهم ما يكون جانبهم «تحدي الشباب» للدخول إلى المواقع الرسمية وبعض الأحيان الدخول إلى مواقع الحسابات من اجل إثبات الذات وغالبا تكون أعمارهم في سن المراهقة.

ثانيا- المحترفون: وهم الأكثر خطورة بين مجرمي الإنترنت، حيث يهدف البعض منهم إلى الاعتداء لتحقيق الكسب غير المشروع المتمثل في الناحية المادية وذلك عبر الدخول في حسابات البنوك والبعض الآخر يدخل من أجل تحقيق أغراض سياسية والتعبير عن وجهة نظرة او فكرة وغالبا اعمار هؤلاء تكون بين 25 و 40 سنة.

ثالثا- الحاقدون: وهم الذين ليس لديهم أي أهداف للجريمة ولا يسعون لمكاسب سياسية او مادية ولكن يتحركون لرغبة في الانتقام والتأثر كالأمور الطائفية.

ما هو مدى التكييف القانوني لمختلف الجرائم الالكترونية التي تجري بالكويت خاصة مع تنوعها خلال الآونة الاخيرة؟

● التكييف القانوني يختلف باختلاف الوقائع التي تم ارتكابها وعلى سبيل المثال: إذا كان الدخول على حسابات الأشخاص لدى البنوك والاستيلاء على أموال منها فإن الوقائع قد تشكل جنحة السرقة وفقا للمادة 221 من قانون الجزاء او جناية السرقة المنصوص عليها بالمواد 222، 223، 224، 225، 226، 227 من قانون الجزاء، حيث تصل العقوبة إلى 3 سنوات، أما اذا كان الدخول الى الحسابات والمواقع الشخصية على شبكة الإنترنت، فإن كان ذلك بنشر عبارات او ألفاظ تشكل قذفا او سبا يكون ذلك معاقبا بالجنحة المؤثمة بالمادتين 209 و210 من قانون الجزاء.

وقد تشكل الأفعال احدى الجنايات المتعلقة بأمن الدولة الخارجي او أمن الدولة الداخلي المنصوص عليها في القانون رقم 1970/31 بتعديل بعض أحكام قانون الجزاء فضلا عن الجنح المؤثمة بالقانون رقم 2011/9 بشأن إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت.

هل الكويت بحاجة إلى تشريع قوانين خاصة لمختلف الجرائم الالكترونية ام هناك قوانين خاصة موجودة حاليا تتعلق بذلك الشأن؟

● لقد بات الوقت ملحا لوجوب تشريع قوانين جديدة بشأن الجرائم الإلكترونية، باعتبارها جرائم مستحدثة بحاجة إلى تشريع خاص يعالج جميع الأفعال التي كشف الواقع العملي عن وجوب تجريمها بما يحفظ صحة وسلامة استخدام الأجهزة الإلكترونية بجميع أنواعها والحفاظ على ما تحتويه من معلومات وبيان كيفية الاستخدام الآمن لهذه المعلومات، لاسيما ان هذه المعلومات على درجة كبيرة من الأهمية لدى الأفراد ولدى الدولة على حد سواء.

ما هي الدوافع الكامنة التي تكون وراء مرتكبي الجرائم الالكترونية بالكويت؟

● هناك دوافع لارتكاب الهاكرز للجرائم غير المشروعة او تشجيع المجرم على ارتكابها وهي دوافع ذاتية كالرغبة في الانتقام أو الطمع أو حب الثراء السريع غير المكلف، وهناك بعض آخر لديه دوافع نفسية كالرغبة في إثبات الذات والتفوق في تعقيد وسائل التقنية، وهناك دوافع اخرى سياسية يحاول من خلالها المجرم الدفاع عن هذه الآراء ضد المعارضين.

لكل جريمة طرق ولكن للجريمة الالكترونية طبيعة خاصة، فهل تحدثنا عنها؟

● بداية الجريمة الالكترونية تتم عبر الدخول غير مصرح به إلى النظام او زراعة الڤيروسات لتدمير الملفات المخزنة او للاستيلاء عن المعلومات الموجودة على الأجهزة الخاصة عبر رسائل البريد الإلكتروني التي تستهدف وضع ڤيروسات او التنصت والاستطلاع على ما بداخل الجهاز، وهو الأمر الذي يتسبب في خسائر مادية خاصة فيما يتعلق بالمؤسسات الاقتصادية مثل البنوك التي تتعرض لسحب أرصدة العملاء بطريقة غير مشروعة.

وهنا لابد من التنوية بأن القوانين الموجودة في الكويت عامة فيما يتعلق بالجرائم الالكترونية وعليه تصل العقوبة في بعض الأحيان إلى 3 سنوات ضمن القواعد العامة للقانون.

ما هي توصياتك تجاه الجهات والسلطات لمواجهة الجرائم الالكترونية بالكويت؟

● ضرورة إيجاد تشريعات خاصة للجرائم الإلكترونية كما هو معمول به في بعض الدول الأجنبية، فنحن نحتاج قوانين خاصة الجرائم المعلوماتية، كونها ازدادت في الآونة الأخيرة وبدأ يتجرأ الهاكرز على الدخول للمصالح والمؤسسات الكويتية فضلا عن التأثير على المواقع الالكترونية للقطاع المصرفي، لذا فهناك ضرورة لتشريع قوانين خاصة لها لحماية القطاعات الاقتصادية والخصوصية بشكل عام.

● محمود فاروق

«الهاكرز» ثلاثة أنواع.. الأبيض والأسود والرمادي أخطرهم

يصنف الهاكرز الى أكثر من نوع وهي:

الهاكرز الأسود وهو الشخص المفسد أو ما يسمى باللغة الانجليزية الـ Black Hat Hacker وهو شخص يعمل على اختراق حسابات أشخاص أو مؤسسات والهدف من ذلك المتعة والتحدي لاثبات مهارته التقنية (ذلك ما كان يحدث في البداية) ولكن في الفترة الأخيرة تحول الكثير من هؤلاء لسرقة معلومات شخصية أو بنكية أو الحصول على معلومات من الضحية تسمح له باختراق ضحية أخرى وعند ذكر أشهر الأمثلة فلابد أن نذكر جوناثان جيمس وكيفن ميتنيك وكيفن بولسن وروبرت موريس تابان وفلاديمير ليفين ويوهان هيلسينجيوس الذين يعتبرون من اشهر الهاكرز.

النوع الثاني ويسمي بالهاكرز الأبيض (الهاكر الأخلاقي) أو الـ White Hat Hacker وهدف هذا الشخص هو تخطي الحماية واختراق المنشآت من أجل كشف الثغرات والبحث عن المشاكل الأمنية وتبليغ المسؤولين عنها وليس استغلالها لهدف شخصي.

النوع الثالث وهو من يجب الحذر منه أكثر من النوع الأول (من وجهه نظري) وهو الهاكرز الرمادي أو ما يسمي Gray Hat Hacker أو المتلون وهو شخص غامض غير محدد اتجاهه لأنه يقف في منطقة حدودية بين الهاكرز الأسود والأبيض فمن الممكن في بعض الحالات ان يقوم بمساعدتك وحالة أخرى تكون هدفه وضحيته القادمة وفي الغالب يقوم هذا النوع عند اكتشاف ثغرة ما بنشرها لعموم الناس بدلا من ابلاغ المسؤولين عنها وممكن أن يقوم بكسر تشفير البرامج والتراخيص الخاصة بالبرامج أو الميديا وأى شيء له علاقة بحقوق النشر ونشرها على الإنترنت بدون مقابل وهناك الكثير من الشخصيات المشهورة التي تنضم لهذا النوع مثل غاري ماكينون وأدريان لامو.

النوع الرابع وهو الهاكر صاحب القبعة الزرقاء أو ما يعرف بـ Blue Hat Hacker فهو شخص يأتي من الخارج وهو متخصص في مجال الحماية ويقدم استشارات أمنية بعد فحص النظام في محاولة لايجاد المشاكل والعلل الأمنية قبل اطلاق النظام في السوق والسبب في تسميته (القبعة الزرقاء) بالتحديد لأن شركة مايكروسوفت (صاحبة اللون الازرق) هي من أوائل الشركات التي فعلت ذلك.

نوع يتواجد بكثرة في الوطن العربي وهو مايسمي بـ Script Kiddie والمقصود من الاسم التحقير من شخص ليس لديه أي معلومات عن الكمبيوتر أو مهارته ضئيلة أو شبة معدومة ويستخدم أدوات أو برامج أو نصوص جاهزة بالاختراق لمهاجمة الآخرين سواء كانت أنظمة كمبيوتر أو شبكات أو تخريب مواقع إلكترونية دون فهم معنى ما يستخدمه أو طريقة عمله.

هاكر Phreaker وهو شخص يقوم باختراق شركات الاتصالات من أجل السرقة أو التجسس على أرقام معينة أو الحصول على خطوط اتصالات غير مدفوعة الثمن أو ما يعرف بـ Free long distance call والأمثلة كثيرة مثل جون درابر ومارك أبيني وديني تيريسي.

نوع آخر وهو ما يطلق عليه النخبة أو الـ Elite Hacker وهو شخص موهوب جدا في الحماية والاختراق وظيفتهم تتمحور حول الكشف عن المشاكل أو الثغرات التي قام بها الهاكرز المخربين (في البنية التحتية للشبكات وأنظمة الكمبيوتر) ومحاولة معالجتها وتتبع المخترقين ويعمل هذا النوع مع الحكومات وشركات الحماية والمؤسسات المهمة والحساسة كالمخابرات والجيش وهكذا والمثال الأشهر اعلاميا سيكون تسوتومو شيمومورا.

المبتدئ ويطلق عليه لقب Hobby Hacker أو Neophyte والفرق بين اللقبين بسيط وهو شخص في أول خطواته في دراسه الاختراق سواء عن طريق كسر تشفير البرامج مدفوعة الأجر وفي الغالب ومع المزيد من الخبرة يتحول هذا الشخص الى أحد الأنواع الثلاثة الأولى كبداية.

النوع المتعلق بالسياسة وهو الـ Hacktivist أو الهاكر السياسي وهو شخص يقوم باختراق مواقع على الانترنت لإظهار دعمه أو نضاله لقضية ما سواء كانت سياسية أو حتى اجتماعية وأشهر مثال على ذلك مجموعة أنونيموس ومجموعة Z Company Hacking Crew وهناك أيضا الكثير من الفرق العربية المعروفة في هذا النوع.

الـ Spy Hacker فهو شخص يتم تعيينه من قبل شخص أو شركة ما لجمع معلومات عن الضحية واختراقه للحصول على معلومات قيمة أو اتلافها وفي المقابل يحصل على مبلغ معين مثل المرتزقة بالضبط وهذا النوع يتواجد بكثرة في أوروبا الشرقية وروسيا والصين.

نوع يندرج تحت النوع الثاني ويطلق عليه لقب Academic Hacker وهو شخص غير مهتم بأنظمة الحماية ولكنه مهتم بالبرمجة وعمل برامج سهلة وذكية وتدرس لطلاب الجامعة أو المعاهد المتخصصة عن الهاكر وكل شيء عنهم سواء أفكارهم أو دراستهم أو الاختراقات التي يقومون بها ويحاول أن يجعل الطلاب يقومون بتطوير وتحسين هذه الادوات والأمثلة كثيرة في أغلب جامعات العالم (ما عدا الجامعات العربية)

الـ Cracker ووظيفته تتمحور في الغالب عند محاولات لكسر أو فك تشفير الحماية الموجودة على المنتجات المدفوعة الأجر ونشرها للعامة بدون مقابل وهو النوع المفضل لدى المستخدمين العرب ولكن الكثير منا لا يفهم أن بعضا من هذه البرامج تجعل منا ضحية حيث من الممكن أن يتم اختراق حاسوبه أو أن يكون منصة للهجوم على ضحية أخرى

نوع آخر وهو Green Hat Hacker أو Newb Hacker وهو باختصار شخص لديه شغف ومحبة لدراسة القرصنة ورغبة في التعلم أكثر وأكثر عنها ولكنه لا يقوم بأى أعمال من القرصنة فقط دراسته تأتي من دافع الفضول.

وهناك أنواع أخرى مثل الـ Spammer وهو شخص يقوم بإرسال رسائل تسويقية لمنتج ما الى ملايين من المستخدمين ولكن لو أرسل ڤيروسات فسيصنف على أنه من النوع الأول ولذلك لابد من الانتباه لهذه التفاصيل الصغيرة وهناك أيضا نوع آخر وهو يصنف تحت تصنيف النوع الأول الا وهو الـ Phisher أو الصياد وهو شخص ينشأ صفحات وهمية تطابق الصفحات الأصلية والغرض من ذلك سرقة بيانات الضحايا وهناك أيضا هاكر ذو القبعة الصفراء (Yellow Hat Hacker) ولكن لو تحدثت عنه سيحدث هناك اختلاط في الأفكار ولكن أستطيع أن أقول أن هذا النوع يشبة النوع الأول والثالث وهناك نوع يطلق عليه اسم Cyberpunk وهو هاكر يستخدم أكثر من طريقة للقيام بعمليات غير قانونية أما آخر نوع فهو الـ Cypherpunk وهو مجموعة تهدف الى تحقيق الخصوصية والأمن للمستخدمين من خلال تشفير بياناتهم وقد ظهرت هذه المجموعة في منتصف الثمانينيات ومازالت موجودة حتى الان.

● منى الدغيمي

القرصنة في أرقام

● يوجد ما يزيد على 403 ملايين من البرمجيات الضارة في عام 2012، في حين كان عددها 286 مليونا عام 2010.

● بحسب آخر الاحصاءات السنوية فإن جرائم القرصنة والاحتيال تكلف العالم 250 مليار دولار سنويا، يصل نصيب منطقة الشرق الأوسط منها نحو 50 مليار دولار.

● قدر اقتصادي سعودي مختص في مكافحة الاحتيال المالي الخسائر المترتبة على عمليات الاحتيال المالي على المستوى العالمي بما يقارب 3,5 تريليونات دولار سنويا، وهو ما يعادل نحو 5٪ من دخل الاقتصاد العالمي المقدر بنحو 70 تريليون دولار.

6 نصائح تجنبك الاحتيال عبر الإنترنت

لا ترد على رسائل البريد الالكتروني التي تطلب معلوماتك الشخصية.

لا تقم بالنقر فوق الروابط المشبوهة، وبدلا من ذلك قم بزيارة مواقع الويب بكتابة محدد موقع المعلومات URL الخاص بها داخل المستعرض الخاص بك.

استخدم كلمات مرور قوية مع ضرورةتغيرها باستمرار.

لا ترسل معلومات شخصية في رسائل البريد الالكترونية المنتظمة. مارس أعمالك مع الشركات التي تعرفها وتثق بها فقط، حتى لا تقوم بتمرير اسمك ومعلوماتك الشخصية للآخرين.

لحماية الكمبيوتر الشخصي الخاص بك: من الضروري استخدام جدار حماية وتحديث الكمبيوتر الخاص بك واستخدام برامج مكافحة الڤيروسات.