

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

طبقات الحماية
والأمن الرقمي

+218 21 361 4115
+218 21 361 4127
+218 21 361 4177
info@nissa.gov.ly
www.nissa.gov.ly
www.cert.gov.ly

وعي المستخدم

رغم التطور الكبير في التقنيات و الأدوات والبرمجيات التي تساعد في حماية المؤسسات والأشخاص .. يظل العنصر البشري هو الحلقة الأضعف في تلك السلسلة ..ولأنه التقنية تتسارع وتيرتها بشكل أكبر من قدرة الإنسان على استيعابها .. فالمخاطر الالكترونية المصاحبة لتلك التقنية تتفاقم لتشكل ثقلاً معلوماتياً وفجوة تحتاج إلى الكثير من الجهد والوقت ..

العديد من المخاطر الإلكترونية حالياً تعتمد بشكل كبير على علم الهندسة الاجتماعية Social Engineering والذي يعني فن اكتشاف نقاط الضعف في شخصية الضحية ،وعند الحديث عن الأنظمة المحوسبة Computing Systems ، فلابد أن نعلم أن هذه الأنظمة لديها العديد من نقاط الضعف Vulnerabilities، ويتم معالجة هذا الضعف من خلال إضافة تحديثات معينة Updates أو استخدام أنظمة أمنية Security Systems أخرى.

وفي المقابل لكي نتمكن من معالجة الثغرات التي تستغلها الهندسة الاجتماعية لخداع الضحايا،فإننا نلجأ إلى زيادة الوعي لدى الأفراد..لأن المؤسسات ببساطة قد تضع حلولاً أمنية بقيم مرتفعة، ثم يحدث الاختراق بنقرة على ملف مصاب، أو قد يتم سرقة بيانات المؤسسة بالكامل ويتمكن منها المنافسين من خلال أحد موظفيها لرابط ملغوم..

فالإنسان جزء من المشكلة ..
و جزء من الحل

طبقات الحماية



الأمن المادي

حماية الأشخاص والممتلكات والبيانات المهمة والمعلومات السرية والشبكات والبرامج والمعدات والمرافق وأصول الشركة التي قد تسبب ضررًا أو خسارة هو ما يدور حوله الأمن المادي في مكان العمل. هناك نوعان من العوامل التي يمكن أن يتأثر بها الأمن، الأول الهجمات الطبيعية مثل الفيضانات والحريق ،وتذبذب الكهرباء ، إلخ. وفي هذه الحالة لن تتعرض البيانات للعبث أو إساءة استخدامها إلا أنه من الصعب جدًا استردادها بعد وقوع هذه الكوارث وقد يتسبب ذلك في فقد دائم لهذه البيانات والثاني هو الهجمات الخبيثة وتشمل الارهاب والتخريب والسرقة.

أصبح الأمان المادي يُمثل تحديًا أكبر في الآونة الأخيرة مقارنة بالعقود السابقة، حيث تسمح بيئة التكنولوجيا والكمبيوتر الآن بحدوث المزيد من الثغرات بسبب زيادة نقاط الضعف وذلك بتوفر أجهزة أكثر حساسية (مثل محركات أقراص USB وأجهزة الكمبيوتر المحمولة والهواتف الذكية والأجهزة اللوحية وما إلى ذلك) والتي تتيح سرقة البيانات بسهولة ويسر . .

وتؤمّن تدابير الأمن المادي الوصول إلى مرافق المؤسسة ومعداتها ومواردها، مما يؤدي إلى إبعاد الغير المصرح لهم بالوصول لتلك المرافق. كما يُساهم في حماية الممتلكات والموظفين من التهديدات مثل السرقة أو الأضرار المادية وحتى التهديدات البيئية.



الجدران النارية

الجدار الناري (Firewall) هو عبارة عن برنامج أو جهاز لفلترة حزم البيانات قبل دخولها لجهاز الكمبيوتر، وكل حزمة ترد من الشبكة المتصل بها جهاز الكمبيوتر تمر عبر هذا الجدار لفحصها، فإن كانت خصائص هذه الحزمة تطابق مواصفات الحزم المراد حجبها والمضمّنة مسبقاً بقاعدة بيانات الجدار، فلا يسمح لهذه الحزمة بالولوج إلى الشبكة أو جهاز الكمبيوتر.

ويمكن أن تتوفر برامج الجدران النارية في صور متنوعة ومنها البرامج الملحقة بأنظمة التشغيل المختلفة ، و برامج أمن الانترنت وأجهزة الجدران النارية الخاصة بالشبكات.ولتحقق الغاية من الجدار الناري فلابد من وضعه في موقع استراتيجي يضمن ألا تخرج المعلومات أو تدخل إلى الشبكة الداخلية إلاّ عن طريقه.



آليات قفل الجهاز

يُخزِّن الجهاز الذكي العديد من المعلومات الحسَّاسة، مثل الصور الشخصية ومعلومات جهات الاتصال والتطبيقات المصرفية لذا من المهم جداً ضبط آلية معينة لقفله (كلمة مرور،نمط،السوار الذكي،بصمة الإصبع،بصمة الوجه...) تساعد كلمة مرور شاشة القفل في حماية المعلومات الخاصة في حالة فقدان الهاتف أو من وصول مستخدم غير مصرَّح له إليه.



مضاد الفيروسات

هنالك العديد من البرمجيات الخاصة بمكافحة الفيروسات، والبعض منها مجانية، ويحتاج هذا النوع من البرامج إلى تحديث (Update) بشكل دائم لكي يتعرف البرنامج على الفيروسات أو أي برمجيات خبيثة أخرى قد تكون أنتجت مؤخراً، فإن لم يتحصل البرنامج المضاد للفيروسات على هذه التحديثات في وقتها فإنه يصبح غير ذو جدوى.



تحديثات نظام التشغيل

باستخدام طريقة التحديث عبر الانترنت لم تعد الشركات تسعى إلى إصدار نسخة جديدة من نظم التشغيل كل بضعة أشهر فنظام التشغيل يمكن أن يعيش لسنوات طويلة طالما تتمكن الشركات المنتجة لها من علاج المشاكل التي تظهر به ومن تقديم خدمات جديدة عن طريق مواقعها على شبكة الإنترنت.

هنالك العديد من التحسينات التي بإمكان تحديثات نظام التشغيل أن توفرها، ومن هذه التحسينات سد الثغرات الأمنية التي يمكن أن تنفذ منها الفيروسات والبرامج الضارة إلى جهاز الكمبيوتر،وعلاج بعض مشاكل البرامج المكونة للنظام والتي من الممكن أن تسبب مشاكل للمستخدم؛ مثل توقف نظام التشغيل عن العمل بطريقة غير طبيعية ،وإضافة خصائص جديدة لأنظمة التشغيل.