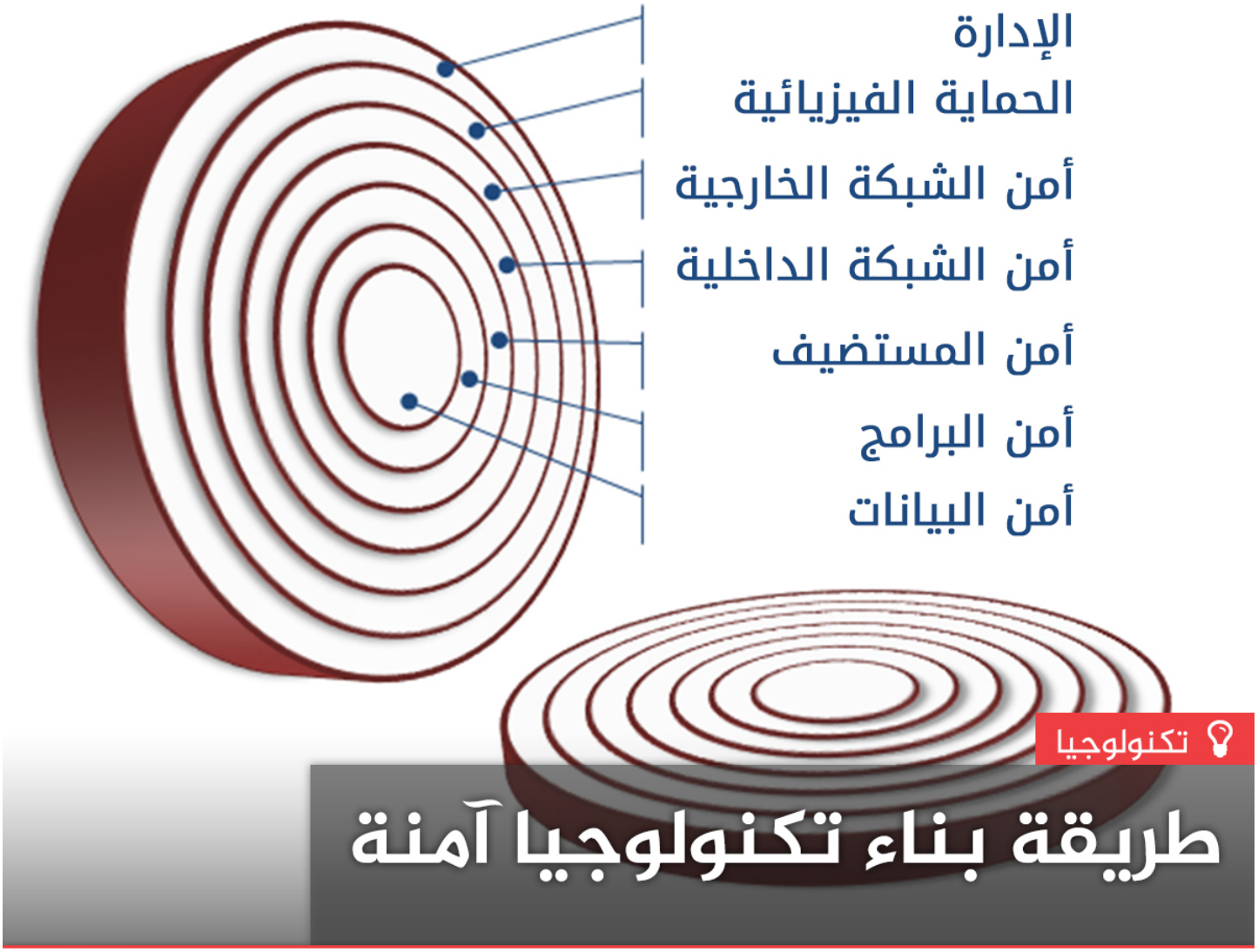
طريقة بناء تكنولوجيا آمنة



في عالم التقنية، هناك مصطلحٌ شائع الاستخدام، وهو مصطلح إطار العمل (**Framework**)، ولكنه عادةً يكون معروفاً على أنه فقط لتسهيل كتابة البرامج للمبرمجين، ولكن حتى للمختصين في أمن المعلومات، هناك العديد من إطارات العمل مثل إطار العمل الأمني "**HIPPA**" المستخدم لحماية البيانات الصحية المتعلقة بالناس في المشافي، تخيل لو أمكن للجميع التلاعب ببيانات التحاليل في المشافي، كم من المرضى كان سيموت سنوياً بسبب هذا التلاعب؟

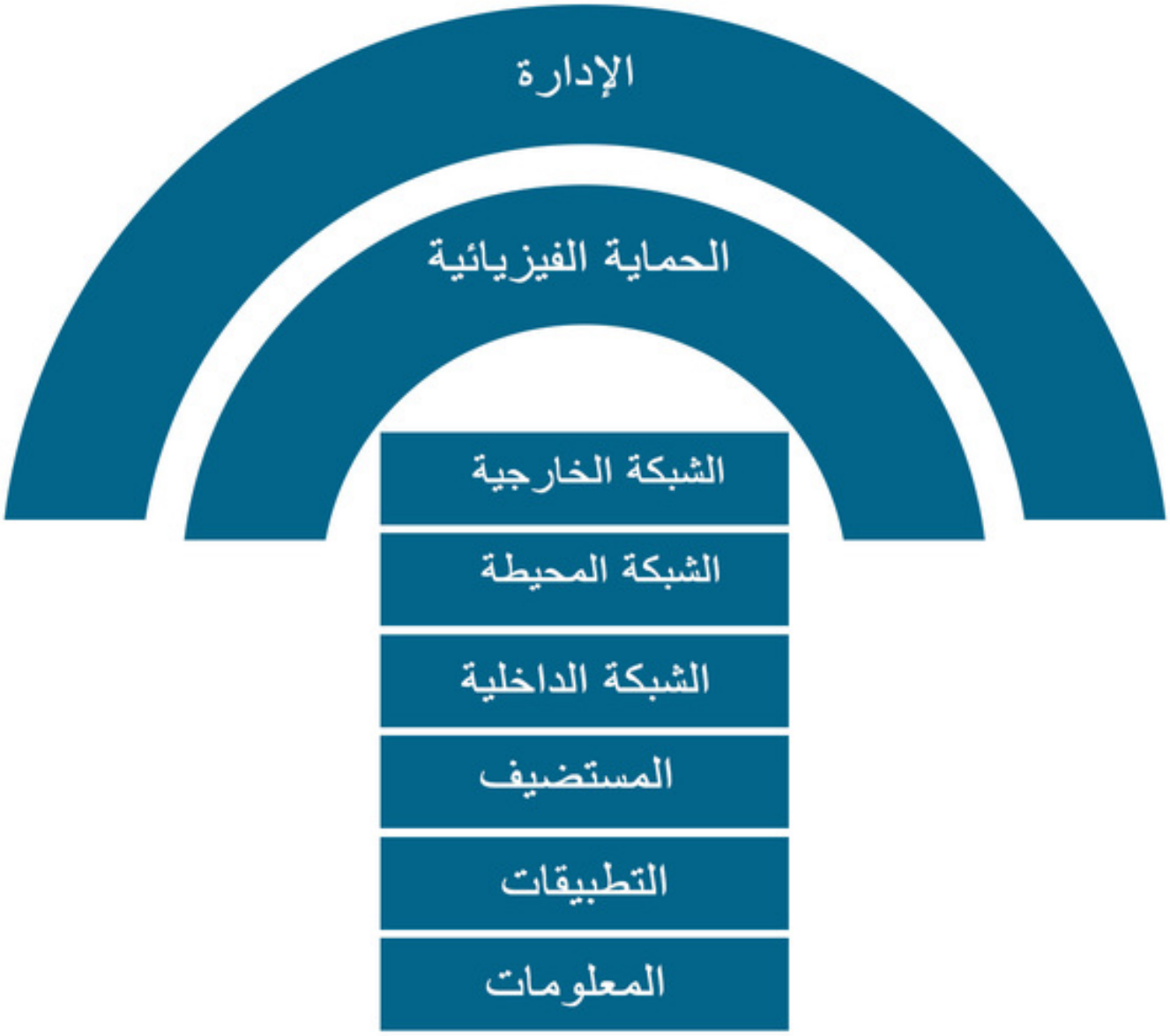
أيضاً لدينا إطار العمل **pci/dss** المختص بحماية بطاقات الائتمان وبياناتها، والذي ساهم بدورٍ كبيرٍ في حماية التجارة الإلكترونية.

اليوم سنركز عن إطار عملٍ عامٍ وشامل، ويمكن تطبيقه على أي نوعٍ من أنواع الشركات أو البرامج أو حتى للاستخدام الشخصي، إنه

يدعى **defense-in-depth** أو الدفاع في العمق.

يبنى هذا المفهوم على أن الأمان يجب أن يقسم إلى عدة طبقات، وفي كل طبقة أمنية هناك العديد من الخيارات المتاحة لحماية التكنولوجيا قبل الانتقال للطبقة التالية.

قسم علماء أمن المعلومات هذا الإطار إلى العديد من الأنواع والتقسيمات المتفرعة، ولكن الأعم والأكثر وضوحاً هو التقسيم التالي:



تمثيل صوري لطبقات الحماية الأمنية

أمن البيانات

يحتفظ معظم الناس والشركات بمعلوماتهم دون أي نوعٍ من أنواع الحماية، وهذا خطر، ورغم أن حماية وتشفير جميع بياناتنا أمرٌ مرهق، ولكن على الأقل البيانات الحساسة والهامة مثل الصور الخاصة والحسابات الضرورية، يجب تشفيرها وحفظها بشكلٍ لا يتيح للآخرين ـ حتى لو حصلوا عليها ـ أن يستفيدوا منها بأي شيء.

أمن التطبيقات

تقنياً، لا يمكننا فتح المعلومات بدون تطبيقاتٍ مخصصةٍ لكل نوعٍ من أنواع الملفات، ولكن ماذا لو كانت بعض التطبيقات هي نفسها السلاح الذي يتم سرقة بياناتنا به؟
منذ عدة سنوات، أُوقفت شركة مشهورة لتحميل التورنت اسمها **limewir** ، وذلك لاستخدامها برنامج يقوم بسرقة البيانات من الجهاز الذي يتم تنصيبه عليه!
ولذلك، عليك الانتباه جيداً للبرامج التي تنصبها على جهازك، ويفضل دائماً استخدام المتاجر المشهورة لتطبيقات الجوال، والمواقع الرسمية لتطبيقات الكمبيوتر، واحذر كل الحذر من التطبيقات المسروقة والكراك.

أمن المستضيف

قد يظن البعض أن الاستضافة هي فقط للمواقع، ولكن جهازك الشخصي هو مستضيفٌ لبياناتك، جوالك مستضيفٌ لصورك، ذاكرة الميموري فلاش الخاصة بك هي مستضيفٌ أيضاً لبياناتك، هل هم محميون جيداً؟
هل تضع صوراً خاصةً على هاتفك لتبكي وتندب عليه إذا ضاع منك؟ كم مرةً سمعت كلمة "ليت جهازي يذهب ولكن فقط البيانات التي عليه تعود أو تمحى"؟
لقد قامت الوحدات الجنائية بالقبض على العديد من عمال الصيانة الذين يسرقون من الأجهزة قبل صيانتها، فهل أنت واثقٌ من شركات الصيانة التي تتعامل معها؟

أمن الشبكة الداخلية

اعتدنا دائماً تشارك شبكة الإنترنت مع الجيران أو الضيوف لدينا، ولكن هل سمعت يوماً بهجوم اسمه **man in the middle attack**.
إنه نوعٌ من السرقة يستخدم برامج لنسخ الماك أدريس الخاص بك **mac address** مما يشتت الراوتر **router** ويجعله يرسل نسخةً من جميع بياناتك للشخص الذي يمتلك نفس الماك أدريس الخاص بك!

ولتجنب هذه الاختراقات احذر دائماً من إعطاء كلمة مرور الإنترنت الخاص بك للأشخاص الغرباء، وضع كلمة سر شديدة القوة والتعقيد للإنترنت لكي لا يستطيع أحد اختراق الشبكة الخاصة بك، وبالتالي سرقة بياناتك.

أمن الشبكة المحيطة

هل ذهبت يوماً إلى فندق أو مطعم فيه خدمة واي فاي مجانية؟
يا سلام! إنه أمر رائع أن تحصل على هذا الإنترنت المجاني خلال جلوسك في الأماكن العامة، ولكن هل تعرف من يتصل معك أيضاً على نفس الشبكة؟ إذاً، عليك بالتفكير ثانيةً في استخدام هذا النوع من الشبكات، فهي قد تكون مفتاحاً لسرقة العديد من بياناتك الهامة مثل معلومات بطاقة الائتمان، وكلمات السر الخاصة بك، بالإضافة إلى ملفاتك الهامة.

أمن الشبكة الخارجية

وهي طبعاً الإنترنت، للأسف لا يمكن حتى اليوم إيجاد طريقةٍ تضمن بها حفظ بياناتك على الإنترنت بشكلٍ كامل، وذلك لأن الثغرات الأمنية لا تلبث أن تظهر في أقوى الشركات وأكثرها موثوقية، وقد سمعنا مؤخراً باختراق حسابات ياهو، ولينكد إن، وغيرها الكثير.

ولكن لتقليل المخاطر، حاول عدم الدخول إلى المواقع غير الموثوقة كالإعلانات المنبثقة والروابط التي تجدها في تعليقات الفيس بوك، مثل اعرف من زار بروفايلك، أو اربح آيفون **8** مجاناً، أنا ربحت واحداً!

الحماية الفيزيائية

وهي الطبقة التي تحيط بكل ما سبق ذكره، فبدونها كل ما سبق وكل ما قمت به من حماية تقنية لا قيمة له.
إن أي شركةٍ لا تمتلك مقومات الحماية الفيزيائية، فإن الوصول إليها وإلى أجهزتها ومعلوماتها سيكون أمراً سهلاً.

تستخدم الشركات اليوم العديد من طبقات الحماية، مثل حساسات الحركة وأجهزة الإنذار، وبطاقة تعريف الموظفين الذكية لحفظ الأجهزة ومنع وصول أشخاص غير مرغوب بهم إلى مبنى الشركة، حيث أن وصول شخصٍ غريبٍ إلى محيط عملك أو شركتك قد يؤدي به إلى تخريب ما يمكنه تخريبه، أو سرقة أجهزة، أو حتى وضع أجهزة تنصت على الشبكة في أي مكانٍ من أماكن تمديدات الشبكة.

الإدارة

وهي الطبقة الأعلى من طبقات الحماية، وبدونها لا يمكن حماية شيء، والمقصود بالإدارة هو توعية الموظفين، وتعليمهم أساليب الحماية والاختراق، فكم من ثغراتٍ أمنيةٍ سببها خيانة داخلية أو جهل المستخدم، الحقيقة أن أكثر من **80%** من الاختراقات سببها جهل المستخدمين.

بدون الإدارة الصحيحة للموظفين وتحديد صلاحياتهم وتوعيتهم، لن نتمكن أبداً من بناء تكنولوجيا آمنة، لذلك ستجد هذه الطبقة هي الأعلى والأهم.

- التاريخ: 2016-12-27
- التصنيف: تكنولوجيا

#تكنولوجيا #أمن معلومات

المصادر

- lynda
- securityintelligence
- academy.delmar

المساهمون

- إعداد
  - عصام عباس

- مُراجعة
  - ريم المير أبو عجيب
- تحرير
  - روان زيدان
- تصميم
  - نور سلمان