

الفصل السابع: الأمن وأنظمة الدفع

I. أمن التجارة الإلكترونية:

1. تعريف أمن للتجارة الإلكترونية:

أمن التجارة الإلكترونية هو مزيج من القوانين، السياسات، التقنيات، والإجراءات التنظيمية التي تهدف إلى حماية كل من المستهلكين والتجار من المخاطر المحتملة في بيئة السوق الرقمية. وهو يتطلب إجراءات متعددة الطبقات تعمل معاً لمنع المخاطر مثل الاحتيال، السرقة الرقمية، التدمير المتعمد، وغيرها من الجرائم التي قد تحدث في المعاملات التجارية الإلكترونية.

2. أبعاد أمن التجارة الإلكترونية: تتضمن ستة جوانب رئيسية:

أ. النزاهة

ب. عدم الإنكار

ت. الأصالة

ث. السرية والخصوصية

ج. التوافر

2. التهديدات الأمنية في بيئة التجارة الإلكترونية:

من منظور التكنولوجيا، هناك ثلاث نقاط ضعف رئيسية عند التعامل مع التجارة الإلكترونية: العميل، والخادم، وخطوط الاتصالات. كل نقطة من هذه النقاط تتعرض لتهديدات معينة يمكن أن تؤثر سلباً على عمليات التجارة الإلكترونية. يتعرض العميل، على سبيل المثال، لأخطار تتعلق بالأمان أثناء استخدام الإنترنت، مثل تحميل البرامج الضارة أو التعرض للاحتيال. أما الخوادم، فهي عرضة للقرصنة أو التلاعب من قبل المهاجمين الذين يستهدفون المواقع الإلكترونية من أجل سرقة البيانات أو تعطيل الخدمة. وفي الوقت نفسه، تشكل قنوات الاتصال عبر الإنترنت وسيلة لحركة البيانات قد تتعرض للاعتراض أو التلاعب.

في هذا القسم، نصف بعض أشكال التهديدات الأمنية الأكثر شيوعاً التي تهدد المستهلكين ومشغلي مواقع التجارة الإلكترونية:

أ. البرمجيات الخبيثة

ب. البرامج غير المرغوب فيها

ت. التصيد الاحتيالي

ث. القرصنة والتخريب الإلكتروني

ج. خرق البيانات

ح. احتيال بطاقات الائتمان

خ. انتحال الهوية

د. التزوير (Spoofing) ، التحويل الاحتيالي (Pharming) ، ومواقع البريد العشوائي (Spam Websites)

ذ. التنصت (Sniffing) وهجمات الرجل في المنتصف (Man-in-the-Middle Attacks)

ر. هجمات حرمان الخدمة (Denial of Service) (DoS) وهجمات حرمان الخدمة الموزعة (Distributed Denial of Service)

ز. الهجمات الداخلية (Insider Attacks)

II. **الحلول التقنية (Technology Solutions)** : سوف يتم في هذا القسم استعراض مجموعة من الأدوات والتقنيات التي تُستخدم لتعزيز حماية البيانات وتأمين العمليات التجارية عبر الإنترنت. إليك توسيع للنقاط الرئيسية التي تناولها القسم:

1. **حماية الاتصالات على الإنترنت**: يتناول هذا الجزء تقنيات التشفير كإحدى الركائز الأساسية لحماية البيانات المتداولة عبر الإنترنت. التشفير يُستخدم لضمان سرية البيانات وعدم قدرتها على الوصول من قبل أطراف غير مخولة.

2. **تأمين الشبكات**: لمنع الهجمات على الشبكات التجارية، يعتمد الأمن على مجموعة من الأدوات مثل:
أ. **جدران الحماية (Firewalls)**: تعمل كخط دفاع أول، تتحكم في حركة البيانات الواردة والصادرة وتمنع الوصول غير المصرح به.

ب. **أنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS)**: تقوم هذه الأنظمة بمراقبة حركة البيانات للكشف عن الأنشطة المشبوهة والتصدي لها.

3. **حماية الخوادم والعملاء**: يتم تطبيق تقنيات الحماية على مستوى الخوادم والأجهزة التي يستخدمها العملاء لضمان عدم تعرضها للاختراق:

أ. **التحديثات الأمنية**

ب. **برامج مكافحة الفيروسات والبرمجيات الخبيثة**

ت. **التشفير من طرف إلى طرف**

III. **السياسات الإدارية، والقوانين العامة المتعلقة بأمن التجارة الإلكترونية:**

1. **السياسات الإدارية**: هي مجموعة من التوجيهات التي تحدد كيفية إدارة المخاطر الأمنية

للتجارة الإلكترونية بشكل استراتيجي. تتضمن هذه السياسات التخطيط، التنفيذ، المراقبة، والتحسين المستمر

لضمان الأمان على مستوى الشركة. يمكن تلخيص الجوانب الرئيسية للسياسات الإدارية في التجارة

الإلكترونية كما يلي:

أ. **خطة إدارة المخاطر**.

ب. **سياسات حماية البيانات**

ت. **التدريب والتوعية الأمنية**

2. **القوانين العامة**: تلعب القوانين العامة دوراً رئيسياً في تنظيم وحماية التجارة الإلكترونية من خلال وضع

إطار قانوني يلزم الشركات باتباع معايير الأمان والخصوصية. بعض النقاط الرئيسية في هذا الجانب تشمل:

أ. **قوانين حماية البيانات والخصوصية**

ب. **قوانين مكافحة الجرائم السيبرانية**

ت. **التشريعات الخاصة بالدفع الإلكتروني**

ث. **تشريعات تنظيم التجارة الرقمية (E-commerce Regulations)**

IV. أنظمة الدفع للتجارة الإلكترونية: تعتبر أنظمة الدفع في التجارة الإلكترونية من العناصر الحيوية التي تؤثر بشكل مباشر على تجربة المستخدم وسهولة إتمام المعاملات. تشمل الأنظمة مجموعة متنوعة من الوسائل التي تلبي احتياجات المستخدمين المختلفة، منها:

1. المعاملات عبر بطاقات الائتمان والخصم
2. المحافظ الرقمية
3. خدمة "اشتر الآن وادفع لاحقاً"
4. العملات الرقمية وتقنية البلوك تشين
5. أنظمة الدفع عبر الهاتف المحمول (