الأكاديمية العربية الدولية
Arab International Academy

أمن المعلومات-2

Information Security-2

م. خليل المحمد

كلية العلوم – ماجستير علم البيانات

الأكاديمية العربية الدولية
Arab International Academy

المحاور

1. مقدمة في أمن المعلومات
2. التهديدات والهجمات الإلكترونية المتقدمة
3. تقنيات الحماية والأمان المتقدمة
4. أمن الشبكات
5. أمن التطبيقات والبرمجيات
6. سياسات الأمن وإدارة الحوادث

المخرجات المتوقعة من المحاضرة

1. **فهم شامل للمفاهيم الأساسية لأمن المعلومات وأهدافه الرئيسية** مثل السرية، السلامة، والتوفر.
2. **التعرف على أنواع التهديدات والهجمات السيبرانية المتطورة**، بما في ذلك البرمجيات الخبيثة، الهندسة الاجتماعية، وهجمات حجب الخدمة.
3. **اكتساب معرفة متقدمة بتقنيات الحماية والأدوات الأمنية** مثل الجدران النارية المتطورة، أنظمة كشف ومنع التسلل، التشفير، وإدارة الهوية.
4. **فهم أهمية أمن الشبكات، البروتوكولات الآمنة، والشبكات الخاصة الافتراضية (VPN)** في تأمين الاتصالات والبيانات.
5. **الوعي بدور سياسات الأمن، إدارة الحوادث، والتوعية التدريبية** في بناء منظومة أمنية متكاملة وفعالة داخل المؤسسات.

مقدمة في أمن المعلومات

أمن المعلومات هو مجال يهدف إلى حماية البيانات من الوصول غير المصرح به، التلف، أو التعديل.

يرتكز أمن المعلومات على ثلاثة مبادئ رئيسية:

- السرية Confidentiality التي تحافظ على سرية المعلومات.
- السلامة Integrity التي تضمن دقة وسلامة البيانات.
- التوفر Availability الذي يضمن إمكانية الوصول للمعلومات عند الحاجة.

في المحاضرة الأولى، تعرفنا على التهديدات الأساسية مثل الفيروسات والهجمات الإلكترونية.

كما تناولنا أهمية اللوائح والمعايير الدولية مثل معيار ISO 27001 لحماية البيانات.

هذا الأساس يؤهلنا لفهم التهديدات المتطورة وكيفية التصدي لها.

مقدمة في أمن المعلومات

أهمية التعمق في تقنيات وأساليب الحماية الحديثة

تزايدت تعقيدات التهديدات السيبرانية مع تطور التكنولوجيا، مما يستدعي تحديث معارفنا باستمرار.

التهديدات الحديثة تشمل هجمات متطورة مثل التصيد الاحتيالي وبرامج الفدية.

أمن المعلومات لا يعتمد فقط على الأدوات، بل يشمل أيضاً السياسات والتوعية البشرية.

تطبيق تقنيات متقدمة مثل التشفير، الجدران النارية المتطورة، وأنظمة كشف التسلل أصبح ضرورة.

التدريب والتوعية المستمرة للعاملين يحمي المؤسسات من الثغرات البشرية.

الالتزام بالمعايير الدولية يعزز الثقة ويحمي البيانات من الاختراقات.

من خلال التعمق في هذه المجالات، يمكننا بناء دفاعات قوية ضد التهديدات الحديثة.

أنواع الهجمات السيبرانية المتطورة

تطورت الهجمات السيبرانية لتصبح أكثر تعقيدًا وتنظيمًا مع الوقت.

الهجمات المتطورة تستهدف مؤسسات محددة بهدف التجسس أو السرقة.

من أبرز هذه الهجمات:

- الهجمات المستمرة المتقدمة APT التي تدوم لفترات طويلة بسرية.
- البرمجيات الخبيثة المتقدمة التي تتجنب اكتشاف أنظمة الحماية.
- هجمات التصيد الاحتيالي المتخصص Spear Phishing التي تستهدف أفراد بعينهم.

هذه الهجمات غالبًا ما تستخدم تقنيات متطورة لجمع المعلومات والتسلل دون كشف.

أنواع الهجمات السيبرانية المتطورة

تشمل الهجمات المتطورة أيضًا:

- هجمات حجب الخدمة الموزعة DDoS التي تعطل الخدمات عبر إغراقها بحركة مرور ضخمة.
- استغلال الثغرات الأمنية غير المعروفة Zero-Day Exploits التي تستهدف أنظمة بدون حلول فورية.
- هجمات الهندسة الاجتماعية المتقدمة التي تستغل الثقة البشرية.

القدرة على فهم هذه الهجمات تعتبر أساسًا لتطوير استراتيجيات دفاعية فعالة.

التدريب المستمر واستخدام تقنيات الحماية الحديثة من أهم سبل المواجهة.

البرمجيات الخبيثة: الفيروسات والديدان

البرمجيات الخبيثة هي برامج تهدف لإلحاق الضرر أو سرقة المعلومات.

الفيروسات: برامج ترفق نفسها بملفات أو برامج وتنتشر عند تشغيلها، تسبب تلف البيانات أو تعطيل النظام.

الديدان: برمجيات تنتشر ذاتيًا عبر الشبكات دون تدخل المستخدم، تستغل الثغرات الأمنية لنشر نفسها بسرعة.

كلا النوعين يستهلكان موارد النظام ويسببان تباطؤ في الأداء وتعطل الخدمات.

مثال: دودة SQL Slammer التي انتشرت عام 2003 وأثرت على الإنترنت بشكل واسع.

فهم آلية عمل هذه البرمجيات يساعد في تطوير استراتيجيات دفاع فعالة.

البرمجيات الخبيثة: برامج الفدية والتروجانات

برامج الفدية Ransomware: تشفر بيانات الضحية وتطلب فدية مالية لفك التشفير، مسببة خسائر مالية كبيرة.

التروجانات Trojans: برامج تبدو شرعية لكنها تحتوي على وظائف خبيثة مثل سرقة البيانات أو فتح ثغرات.

برامج الفدية مثل WannaCry أثرت على مؤسسات حيوية عالمياً، منها مستشفيات وأنظمة حكومية.

التروجانات تُستخدم في سرقة المعلومات المالية وحسابات المستخدمين البنكية.

الوقاية تشمل تحديث الأنظمة، النسخ الاحتياطي، والتوعية الأمنية للموظفين.

تتطلب مواجهة هذه البرمجيات أدوات وتقنيات متقدمة للدفاع والكشف المبكر.

هجمات الهندسة الاجتماعية: مفهومها وأساسياتها

الهندسة الاجتماعية تعتمد على استغلال الجانب البشري لخداع الأفراد.

تهدف إلى الحصول على معلومات حساسة عبر خداع المستخدمين بدلاً من اختراق الأنظمة.

التصيد الاحتيالي Phishing: رسائل بريد إلكتروني أو روابط تبدو شرعية لخداع المستخدم.

يتم فيها طلب معلومات مثل كلمات المرور أو بيانات البطاقة البنكية.

التصيد العشوائي غالبًا ما يستهدف أعدادًا كبيرة من الأشخاص.

الوعي الأمني هو خط الدفاع الأول ضد هذه الهجمات.

التصيد الاحتيالي المتخصص Spear Phishing وأساليبه

Spear Phishing هجوم موجه بدقة لشخص أو جهة معينة.

يستخدم معلومات شخصية لجعل الرسائل تبدو موثوقة ومقنعة.

يستهدف المسؤولين التنفيذيين أو الموظفين ذوي الصلاحيات العالية.

يمكن أن يؤدي إلى سرقة بيانات هامة أو فتح ثغرات داخل المؤسسة.

أساليب متقدمة تشمل استخدام روابط مزيفة أو مرفقات خبيثة.

الحماية تشمل التحقق من المرسل، التدريب الأمني، واستخدام المصادقة متعددة العوامل.

هجمات حجب الخدمة الموزعة DDoS – التعريف وآلية العمل

هجمات DDoS تستهدف تعطيل الخدمات عبر إغراق الخوادم بطلبات زائدة.

يتم تنفيذ الهجوم من عدة أجهزة مخترقة (بوتنت) موزعة جغرافيًا.

الهدف هو استنزاف موارد النظام وتعطيل الخدمة للمستخدمين الشرعيين.

أنواع الهجمات تشمل استنزاف النطاق الترددي، استنزاف الموارد، وهجمات طبقة التطبيق.

هجمات DDoS تكون صعبة الاكتشاف والتصدي بسبب توزيع مصادرها.

هذه الهجمات قد تؤدي إلى خسائر مالية وسمعة سيئة للمؤسسات.

طرق التخفيف من هجمات DDoS

1. استخدام جدران نارية متقدمة وأنظمة كشف الهجمات.
2. توزيع الحمل عبر خوادم متعددة Load Balancing .
3. الاعتماد على خدمات الحماية السحابية المتخصصة مثل Cloudflare و Akamai
4. تحليل حركة المرور بشكل مستمر للكشف المبكر عن الهجمات.
5. تكوين إعدادات الشبكة لمنع استغلال الثغرات مثل الحد من الاتصالات المفتوحة
6. أهمية التخطيط المسبق والاستعداد للحوادث.

الجدران النارية التقليدية Traditional Firewalls

الجدار الناري هو خط الدفاع الأول لحماية الشبكات من الوصول غير المصرح به.

الجدار الناري التقليدي يعتمد على تصفية الحزم بناءً على عناوين IP، المنافذ، وبروتوكولات الاتصال.

يوفر حماية أساسية ويمنع حركة المرور غير المرغوب فيها.

لا يستطيع فحص محتوى الحزم أو التعرف على التطبيقات داخل الشبكة.

محدود في مواجهة الهجمات المتطورة التي تستخدم تقنيات التمويه.

غالبًا ما يُستخدم في الشبكات الصغيرة أو كجزء من بنية أمان أكبر.

الجدران النارية من الجيل التالي Next-Generation Firewalls – NGFW

NGFW هو جدار ناري متطور يجمع بين الحماية التقليدية ووظائف كشف ومنع التسلل.

يستخدم فحصًا عميقًا للحزم DPI لتحليل محتوى البيانات.

قادر على التعرف على التطبيقات والسيطرة عليها حتى لو استخدمت منافذ غير قياسية.

مدمج مع أنظمة كشف ومنع التسلل IDS/IPS .

يدعم التحديثات التلقائية لمواجهة التهديدات الجديدة.

يوفر تحكمًا دقيقًا في السياسات الأمنية بناءً على المستخدمين والتطبيقات.

أنظمة كشف التسلل IDS وأنظمة منع التسلل IPS

أنظمة كشف التسلل IDS ترصد النشاطات المشبوهة في الشبكة أو الأجهزة:

تقوم بالإبلاغ عن محاولات الهجوم أو النشاطات غير الطبيعية.

لا تمنع الهجمات بشكل مباشر بل تكتفي بالكشف والتنبيه.

أنظمة منع التسلل IPS تتخطى الكشف لتمنع الهجمات تلقائيًا:

تقوم بحظر حركة المرور الخبيثة وإيقاف الهجمات فوراً.

تعمل على تحسين أمان الشبكة من خلال التدخل الفوري.

كل منهما ضروري لتعزيز الحماية الأمنية.

تكامل IDS/IPS مع الجدران النارية

الجدران النارية تراقب حركة المرور وفق قواعد ثابتة (IP، منافذ).

أنظمة IDS/IPS توفر فحصًا أعمق لحركة المرور وتحليلًا للسلوك.

في الجدران النارية من الجيل التالي NGFW ، تدمج IDS/IPS لتوفير حماية متقدمة.

التكامل يسمح بالكشف المبكر ومنع الهجمات بفعالية.

يساعد في تقليل الإنذارات الكاذبة وتحسين سرعة الاستجابة.

يشكل هذا التكامل طبقة أمان متعددة ومتكاملة للشبكات.

التشفير: المفاهيم الأساسية والمتماثل

التشفير هو تحويل البيانات إلى صيغة غير قابلة للقراءة إلا لمن يملك المفتاح.

التشفير يحمي السرية وسلامة البيانات أثناء التخزين والنقل.

التشفير المتماثل يستخدم مفتاحًا واحدًا للتشفير وفك التشفير.

مزايا التشفير المتماثل: سرعة الأداء وكفاءة التشفير لكميات كبيرة من البيانات.

عيوبه: تحديات في تبادل المفتاح بأمان بين الأطراف.

أمثلة على خوارزميات متماثلة: AES، DES.

التشفير اللا متماثل والشهادات الرقمية

التشفير اللا متماثل يستخدم زوجًا من المفاتيح: عام وخاص.

المفتاح العام لتشفير البيانات، والخاص لفك التشفير، مما يحل مشكلة تبادل المفاتيح.

يستخدم في التوقيعات الرقمية لضمان صحة البيانات.

الشهادات الرقمية تصدرها جهات موثوقة CA لتوثيق هوية المستخدم أو الموقع.

تساعد الشهادات في تأمين الاتصالات عبر بروتوكولات مثل SSL/TLS.

معيار الشهادات الشائع: X.509.

بروتوكول SSL/TLS: تأمين الاتصال عبر الإنترنت

SSL وTLS بروتوكولات توفر اتصالًا مشفرًا بين العميل والخادم.

TLS هو النسخة المطورة والأكثر أمانًا من SSL.

تعمل من خلال مصافحة أمان Handshake تتبادل فيها المفاتيح وخوارزميات التشفير.

تستخدم التشفير اللا متماثل لتبادل مفتاح الجلسة بأمان.

بعد المصافحة، يتم تشفير البيانات باستخدام التشفير المتماثل لضمان السرعة والسرية.

يُستخدم بروتوكول HTTPS لحماية تصفح الويب وخاصة المعاملات الحساسة.

بروتوكول IPsec: تأمين طبقة الشبكة

IPsec هو مجموعة بروتوكولات توفر أمانًا على مستوى طبقة الشبكة.

يضمن التوثيق، التشفير، وسلامة البيانات المرسلة عبر الشبكة.

يتضمن بروتوكولات AH مصادقة البيانات و ESP تشفير المحتوى .

يعمل في وضع النقل Transport Mode أو النفق Tunnel Mode .

يُستخدم بشكل واسع في شبكات VPNلتأمين الاتصالات بين المواقع أو المستخدمين.

يوفر حماية شاملة لحركة مرور الإنترنت دون الحاجة لتغيير التطبيقات.

إدارة الهوية والتحكم في الوصول IAM

IAM هو نظام يضمن أن الأشخاص المناسبين يمكنهم الوصول إلى الموارد الصحيحة.

يشمل إنشاء وإدارة الهويات، المصادقة، التفويض، والتدقيق.

يساعد في تحديد الصلاحيات بناءً على الأدوار والوظائف.

يقلل من مخاطر الوصول غير المصرح به.

يساهم في الامتثال للمعايير والقوانين الأمنية.

يدعم إدارة السياسات الأمنية والتحديثات المستمرة.

أنظمة المصادقة متعددة العوامل MFA

MFA تتطلب أكثر من شكل واحد لإثبات الهوية.

تشمل عوامل المعرفة (كلمة المرور)، الامتلاك (رمز على الهاتف)، والعوامل البيولوجية (بصمة).

تزيد من صعوبة اختراق الحسابات حتى لو تم كشف كلمة المرور.

تُستخدم في الأنظمة الحساسة مثل البنوك والخدمات الحكومية.

تحسين كبير في أمان الدخول الإلكتروني.

جزء أساسي من استراتيجيات IAMالحديثة.

الأكاديمية العربية الدولية
Arab International Academy

اسئلة

السؤال 1: ما هي المبادئ الأساسية لأمن المعلومات

السؤال 2: ما الفرق بين الهجمات السيبرانية المتطورة مثل APT وبرمجيات الفدية؟

السؤال 3: ما هي الفرق بين الجدار الناري التقليدي والجدار الناري من الجيل التالي NGFW ؟

السؤال 4: كيف تعمل أنظمة كشف ومنع التسلل IDS/IPS مع الجدران النارية لتعزيز الأمان؟

السؤال 5: ما دور التشفير اللا متماثل والشهادات الرقمية في تأمين الاتصالات؟

الأجوبة

الإجابة 1 :

المبادئ الأساسية لأمن المعلومات هي:

السرية Confidentiality: ضمان عدم وصول المعلومات إلى غير المصرح لهم.

السلامة Integrity: ضمان عدم تعديل أو تلف البيانات بشكل غير مصرح به.

التوفر Availability: التأكد من توفر المعلومات والخدمات للمستخدمين المصرح لهم عند الحاجة.

الإجابة 2 :

الهجمات المستمرة المتقدمة APT : هجمات مخططة تستهدف مؤسسات معينة وتستمر لفترات طويلة بهدف التجسس أو سرقة المعلومات.

برمجيات الفدية Ransomware : برامج خبيثة تشفر بيانات الضحية وتطلب فدية مالية لفك التشفير، وتسبب أضرارًا مالية مباشرة.

الأجوبة

الإجابة 3 :

- **الجدار الناري التقليدي:** يراقب حركة المرور بناءً على عناوين IP والمنافذ فقط، ولا يحلل محتوى البيانات.
- **جدار ناري من الجيل التالي NGFW:** يقوم بفحص عميق للحزم، يتعرف على التطبيقات، ويشمل أنظمة كشف ومنع التسلل، مما يوفر حماية متقدمة.

الإجابة 4 :

- أنظمة IDS تكتشف النشاطات المشبوهة وترسل تنبيهات لكنها لا تمنعها مباشرة.
- أنظمة IPS تمنع الهجمات تلقائيًا عبر حظر حركة المرور الخبيثة.

عند دمجها مع الجدران النارية، توفر حماية متعددة الطبقات، حيث تتحكم الجدران النارية بالوصول بينما تراقب أنظمة IDS/IPS السلوك بشكل أعمق وتتصرف فورًا.

الإجابة 5 :

التشفير اللا متماثل يستخدم زوجًا من المفاتيح (عام وخاص) لتبادل البيانات بأمان دون الحاجة لمشاركة المفتاح السري.
الشهادات الرقمية تصدرها جهات موثوقة CA لتوثيق هوية الطرف المستقبل، وتساعد في بناء اتصال آمن عبر بروتوكولات مثل SSL/TLS

أساسيات أمن الشبكات المحدثة – الأهداف والمكونات الأساسية

أمن الشبكات هو حماية البنية التحتية الرقمية من التهديدات المختلفة لضمان سلامة المعلومات.

الأهداف الرئيسية لأمن الشبكات:

- السرية Confidentiality: حماية البيانات من الوصول غير المصرح به.
- السلامة Integrity: ضمان عدم تعديل أو تلف البيانات.
- التوفر Availability: توفير إمكانية الوصول للمستخدمين المصرح لهم بشكل مستمر.

مكونات أمن الشبكات المحدثة:

مراقبة حركة الشبكة وتحليل البيانات لاكتشاف النشاطات غير الطبيعية.

جدران نارية من الجيل التالي NGFW لفحص الحزم بشكل عميق.

أنظمة كشف ومنع التسلل IDS/IPS للكشف الفوري عن الهجمات.

أساسيات أمن الشبكات المحدثة – التحديات وأفضل الممارسات

التحديات الحديثة في أمن الشبكات:

- تهديدات معقدة مثل الهجمات المستمرة المتقدمة APT وبرامج الفدية.
- انتشار الأجهزة المحمولة وإنترنت الأشياء IoT وزيادة سطح الهجوم.
- الانتقال إلى الحوسبة السحابية يفرض متطلبات أمنية جديدة.

أفضل الممارسات:

تبني نهج الدفاع متعدد الطبقات Defense in Depth .

تدريب مستمر للموظفين على التهديدات الأمنية.

استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي للكشف المبكر.

تحديث الأنظمة والبرمجيات بشكل دوري.

البروتوكولات الآمنة: الأساسيات وأهميتها

تُعد البروتوكولات الآمنة العمود الفقري لحماية البيانات أثناء انتقالها عبر الشبكات، خصوصًا في بيئة الاتصالات عن بُعد.

تحمي هذه البروتوكولات البيانات من التنصت، التعديل، والاعتراض.

تشمل البروتوكولات الأساسية: SSH، HTTPS، وIPsec.

SSH يوفر قناة مشفرة للوصول الآمن إلى الأجهزة عن بُعد.

HTTPS يؤمن تصفح الإنترنت عبر تشفير اتصال المتصفح بالموقع.

IPsec يؤمن طبقة الشبكة بتشفير وتوثيق حركة البيانات.

التطبيق الصحيح لهذه البروتوكولات ضروري لضمان سرية وسلامة الاتصالات.

أمن الاتصالات عن بُعد: التحديات وأفضل الممارسات

الاتصالات عن بُعد تواجه تحديات أمنية كبيرة بسبب استخدام الشبكات العامة وغير المؤمنة.

التنصت والاعتراض من أبرز التهديدات.

انتحال الهوية وهجمات الرجل في الوسط تهدد سلامة البيانات.

أفضل الممارسات تشمل استخدام VPN لتشفير الاتصال.

تطبيق المصادقة متعددة العوامل MFA لتعزيز أمان الدخول.

تحديث البرمجيات بانتظام لسد الثغرات الأمنية.

توعية المستخدمين بأهمية الأمن السيبراني في بيئة العمل عن بُعد.

الحماية الشاملة تعتمد على الجمع بين التكنولوجيا والتوعية البشرية.

تهديدات أمن الشبكات اللاسلكية

الشبكات اللاسلكية توفر سهولة في الاتصال لكنها عرضة لمخاطر أمنية خاصة.

التنصت على الإشارات اللاسلكية وسرقة البيانات.

الوصول غير المصرح به عبر نقاط وصول ضعيفة الحماية.

هجمات الرجل في الوسط التي تعترض وتعدل الاتصالات.

نقاط الوصول المزيفة Rogue Access Points لخداع المستخدمين.

هجمات حجب الخدمة DoS لإغراق الشبكة بالطلبات الزائدة.

تتطلب هذه التهديدات فهماً دقيقاً واتخاذ تدابير وقائية فعالة.

التدابير الوقائية لأمن الشبكات اللاسلكية

استخدام تشفير WPA3 كأحدث معايير الحماية.

إخفاء اسم الشبكة SSID لمنع اكتشافها بسهولة.

تطبيق قوائم التحكم في الوصول MAC Filtering .

تحديث البرامج الثابتة Firmware لنقاط الوصول بانتظام.

فصل شبكات الضيوف عن الشبكة الأساسية.

مراقبة الشبكة لاكتشاف الأجهزة والسلوكيات المشبوهة.

توعية المستخدمين بأهمية الحذر عند الاتصال بالشبكات العامة.

هذه الإجراءات تعزز أمن الشبكات اللاسلكية وتحمي البيانات من التهديدات.

مفهوم الشبكات الخاصة الافتراضية VPN - انواعها

الشبكة الخاصة الافتراضية VPN: تتيح إنشاء اتصال آمن ومشفر عبر الإنترنت و تسمح للمستخدمين بالوصول إلى شبكة خاصة وكأنهم متصلون بها محليًا.

الهدف الأساسي: حماية الخصوصية والبيانات أثناء التنقل كما تحمي الاتصالات من التنصت والتدخل غير المصرح به.

تستخدم تقنية التشفير لإنشاء نفق آمن بين الجهاز والشبكة و تعد أداة رئيسية للعمل عن بُعد وحماية البيانات في الشبكات العامة.

الأنواع:

VPN الوصول عن بُعد: يتيح للأفراد الاتصال بالشبكة الداخلية من أي مكان.

VPNالشبكة إلى الشبكة: يربط شبكات فرعية متعددة بأمان عبر الإنترنت.

يستخدم VPN في المؤسسات لتأمين البيانات وحماية الخصوصية.

بروتوكولات شائعة: IPsec، SSL/TLS، L2TP. أهمية تطبيق مصادقة متعددة العوامل مع VPN لزيادة الأمان.

دراسة حالة: استخدام VPN في المؤسسات أثناء جائحة كورونا لتأمين العمل عن بُعد.

مخاطر أمن التطبيقات: حقن SQL (SQL Injection)

حقن SQL ثغرة تسمح للمهاجم بإدخال أوامر ضارة في استعلامات قاعدة البيانات و تحدث عندما لا يتم التحقق من صحة المدخلات بشكل صحيح.

تمكن المهاجم من استعراض، تعديل، أو حذف بيانات حساسة و قد تؤدي إلى اختراق كامل للنظام أو سرقة بيانات المستخدمين.

أمثلة على الهجوم: إدخال كود SQL في حقول البحث أو تسجيل الدخول.

طرق الوقاية: استخدام الاستعلامات المحضرة Prepared Statements والتحقق من المدخلات.

يجب تنفيذ سياسات أمان صارمة لقواعد البيانات.

مخاطر أمن التطبيقات: XSS وCSRF

XSS البرمجة عبر المواقع: تسمح بحقن أكواد جافا سكريبت خبيثة في صفحات الويب.

تنقسم إلى XSS المخزنة والمعكوسة، تؤدي إلى سرقة بيانات الجلسة وتنفيذ هجمات احتيالية.

CSRF تزوير طلبات المواقع تخدع المستخدم لإرسال طلبات غير مرغوب فيها أثناء تسجيل الدخول.

قد تؤدي إلى تغيير الإعدادات أو تنفيذ عمليات مالية دون إذن.

الوقاية من XSS: تصفية المدخلات وترميز المخرجات، واستخدام سياسات الأمان للمحتوى.

الوقاية من CSRF: استخدام رموز التحقق CSRF Tokens والتحقق من مصادر الطلبات.

التدريب الأمني وتحديث البرمجيات يقللان من مخاطر هذه الثغرات.

اختبار الاختراق: التعريف والمنهجيات

اختبار الاختراق: هو محاكاة لهجوم حقيقي على نظام لكشف الثغرات.

الهدف: تقييم مستوى الأمان وتحسينه قبل استغلال المهاجمين.

خطوات المنهجية:

1. جمع المعلومات Reconnaissance عن الهدف.
2. المسح والفحص Scanning للكشف عن الأنظمة والخدمات.
3. الاستغلال Exploitation لتأكيد وجود الثغرات.
4. رفع الامتيازات Privilege Escalation لتعزيز النفوذ.
5. الحفاظ على الوصول Maintaining Access لفترة طويلة.
6. التقرير Reporting بتفاصيل الثغرات والتوصيات.

أدوات اختبار الاختراق الأساسية

Nmap : لفحص الشبكات واكتشاف الأجهزة والخدمات.

Metasploit : منصة لاستغلال الثغرات بشكل تلقائي.

Burp Suite : اختبار أمان تطبيقات الويب وتحليل الطلبات.

OWASP ZAP : أداة مفتوحة المصدر لفحص الثغرات في الويب.

Wireshark : تحليل حزم البيانات المارة عبر الشبكة.

Nessus : ماسح ثغرات شامل للكشف عن نقاط الضعف.

اختيار الأدوات المناسبة يعتمد على طبيعة النظام والهدف من الاختبار.

مفهوم وأهمية خطط استجابة الحوادث – مراحل الاعداد

خطط استجابة الحوادث: هي إجراءات منظمة للتعامل مع الحوادث الأمنية و تهدف إلى تقليل الأضرار وتأمين استمرارية العمل.

- تمكن المؤسسة من التعرف السريع على الحوادث ومواجهتها بفعالية و تحسن التنسيق بين فرق الأمن والإدارة والأطراف المعنية.
- تساعد في الالتزام بالمعايير القانونية والتنظيمية و توفر آليات لتوثيق الحوادث وتحليلها لاستخلاص الدروس.
- تُعتبر جزءًا أساسياً من استراتيجية الأمن الشاملة.

مراحل إعداد وتنفيذ خطة استجابة الحوادث

1. التحضير: تجهيز الفرق، الأدوات، والتدريب.
2. الكشف والتحديد: رصد الحوادث وتقييمها.
3. الاحتواء: منع انتشار الحادث وتحديد نطاقه.
4. الإزالة: القضاء على مصدر الهجوم وتصحيح الثغرات.
5. الاستعادة: إعادة الأنظمة والخدمات للعمل بشكل طبيعي.
6. التعلم: مراجعة الحادث وتحسين الخطط المستقبلية.
7. التدريبات الدورية تعزز جاهزية الفرق وتقلل من تأثير الحوادث.

أهمية التوعية والتدريب الأمني – الأساليب والمواضيع

أهمية التوعية والتدريب الأمني:

العامل البشري هو أحد أهم عناصر أمن المعلومات وأضعفها في نفس الوقت كما ان التوعية تقلل من الأخطاء البشرية التي تؤدي إلى حوادث أمنية.

تدريب الموظفين يزيد من فهمهم للتهديدات وأساليب التصدي لها و يعزز الالتزام بسياسات الأمن واستخدام الأدوات بشكل صحيح ويرفع من قدرة الموظفين على التعرف على محاولات التصيد والهجمات الاجتماعية و يدعم الامتثال للمعايير والتشريعات الأمنية و يخلق ثقافة أمنية داخل المؤسسة.

أساليب التدريب الأمني

- التدريب الحي والدورات الإلكترونية لزيادة الوصول والمرونة.
- محاكاة هجمات التصيد الاحتيالي لاختبار ردود الفعل.
- التركيز على أساسيات أمن المعلومات وسياسات الشركة.

مواضيع التدريب الأمني

1. تعليم استخدام كلمات مرور قوية والمصادقة متعددة العوامل.
2. التوعية بأهمية تحديث البرمجيات واستخدام الشبكات الآمنة.
3. تعليم طرق التبليغ عن الحوادث الأمنية بشكل سريع وفعال.
4. برامج تدريب مستمرة لمواكبة التهديدات المتجددة.

الأكاديمية العربية الدولية
Arab International Academy

أسئلة

السؤال 1: ما هي الأهداف الأساسية لأمن الشبكات المحدثة؟

السؤال 2: ما الفرق بين بروتوكولات SSH وVPN في تأمين الاتصالات عن بُعد؟

السؤال 3: ما هي أهم أنواع الثغرات الأمنية في تطبيقات الويب مثل XSS وSQL Injection؟ وكيف يمكن الوقاية منها ؟

السؤال 4: ما هي مراحل اختبار الاختراق الرئيسية؟

السؤال 5: ما هي أهمية سياسات أمن المعلومات وخطط استجابة الحوادث في المؤسسات؟

الأجوبة

الإجابة1 :

السرية Confidentiality : حماية البيانات من الوصول غير المصرح به.

السلامة Integrity : ضمان دقة البيانات وعدم تعديلها أو تلفها.

التوفر Availability : ضمان استمرارية الوصول إلى الشبكة والخدمات.

الإجابة 2 :

- **SSH :** يوفر قناة اتصال مشفرة للوصول الآمن إلى الأجهزة عن بُعد، غالبًا يستخدم لإدارة الخوادم.
- **VPN :** ينشئ نفقًا مشفرًا بين المستخدم والشبكة الخاصة، يحمي جميع الاتصالات ويستخدم لتأمين تصفح الإنترنت والعمل عن بُعد.

الإجابة 3 :

- **XSS :** هجوم يحقن أكواد جافا سكريبت ضارة داخل صفحات الويب لخداع المستخدمين.
- **SQL Injection :** ثغرة تسمح بحقن أوامر SQL ضارة لاستغلال قاعدة البيانات.

الوقاية :التحقق من صحة المدخلات، ترميز المخرجات، استخدام استعلامات محضرة، وتطبيق سياسات أمان صارمة.

الأجوبة

الإجابة 4 :

1. جمع المعلومات Reconnaissance . 2. المسح والفحص Scanning . 3. الاستغلال Exploitation .

4. رفع الامتيازات Privilege Escalation . 5.الحفاظ على الوصول Maintaining Access . 6. التقرير Reporting .

الإجابة 5 :

سياسات أمن المعلومات: توفر إطار عمل واضح لحماية البيانات وتحدد المسؤوليات والإجراءات الواجب اتباعها.

خطط استجابة الحوادث: تضمن استعداد المؤسسة للتعامل السريع والفعال مع الحوادث الأمنية لتقليل الأضرار واستعادة العمل بأسرع وقت ممكن.

روابط خارجية

عنوان الفيديو	الرابط
دورات مجانية ومدفوعة لتعلم مهارات الأمن السيبراني.	https://www.cybrary.it/
Nmap أداة مسح الشبكات	https://nmap.org/
منصة لاختبار الاختراق تحتوي على مكتبة كبيرة من الثغرات.	https://www.metasploit.com/

المراجع

- Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice*. Pearson.
- مرجع شامل يغطي أساسيات التشفير، البروتوكولات الأمنية، وأمن الشبكات.
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security*. Cengage Learning.
- كتاب مهم يتناول مبادئ أمن المعلومات، التهديدات، والتقنيات الأمنية.
- Shon Harris. (2019). *CISSP All-in-One Exam Guide*. McGraw-Hill Education.
- دليل متكامل لموضوعات الأمن السيبراني يشمل إدارة الهوية، السياسات، واستجابة الحوادث.
- OWASP Foundation. (2023). *OWASP Top Ten Web Application Security Risks*. Retrieved from https://owasp.org/www-project-top-ten/
- المصدر الرسمي لأهم الثغرات في تطبيقات الويب وأساليب الوقاية منها.
- National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*.
- وثيقة إطار العمل الأمني المعتمد دولياً لتحسين الأمن السيبراني.
- ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization.
- المعيار الدولي لإدارة أمن المعلومات.
- Kaspersky. (2024). *Understanding Ransomware: How It Works and How to Protect Yourself*. Retrieved from https://www.kaspersky.com/resource-center/threats/ransomware
- شرح تفصيلي عن برامج الفدية وأساليب الحماية.
- Symantec Corporation. (2023). *Internet Security Threat Report*.
- تقرير سنوي عن التهديدات السيبرانية الحديثة.

خاتمة

آمل ان تكونوا قد حققتم الفائدة
شكرا لكم