السلام عليكم صديقي 🌟

طلبك هو **تلخيص كل صفحة على حدة** من ملف PDF المرفوع والذي يحتوي على أكثر من 100 صفحة.

لقد بدأت الآن بتلخيص **الصفحة رقم 1 (وهي الصفحة رقم 138 في الملف)**، وإليك ملخصها:

**✅ تلخيص الصفحة 1 من الملف (صفحة رقم 138):**

**الوحدة 11 – الأمن السيبراني وإدارة الحوادث**

* تتناول الصفحة مقدمة حول **تهديدات الأمن السيبراني**، مع التركيز على الأجهزة الرقمية مثل الحواسيب والهواتف المحمولة التي تتعرض لتهديدات متعددة.
* **أنواع التهديدات:**
  + **داخلية:** مثل موظفين غير راضين يقومون بحذف أو تسريب بيانات حساسة، أو يحصلون على وصول غير مصرح به.
  + **خارجية:** تأتي من خارج المؤسسة وتتنوع بين برامج خبيثة، فيروسية، أو هجمات إلكترونية مباشرة.
* **أمثلة على التهديدات الداخلية:**
  + حذف بيانات أو تخريب الأجهزة من قبل موظف مفصول.
  + الوصول غير المشروع إلى معلومات مثل كشوف الرواتب.
  + السماح للزوار أو الشركاء بالوصول إلى أنظمة لا يجب الوصول لها.
* **مخرجات التعلم:**
  + فهم التهديدات والثغرات الأمنية.
  + استكشاف أثر الأنظمة المتصلة بالشبكة.
  + إعداد خطة حماية للأمن السيبراني.
  + فهم كيفية جمع الأدلة الجنائية بعد وقوع الحوادث.

**✅ تلخيص الصفحة 2 من الملف (صفحة رقم 139):**

**تابع الوحدة 11 – الأمن السيبراني وإدارة الحوادث**

**🔸 التهديدات الخارجية:**

* توضح الصفحة أنواع **البرمجيات الخبيثة** التي تُستخدم في الهجمات:

**1. برامج التجسس:**

* + تجمع معلومات عن المستخدم دون إذنه (مثل عادات التصفح).
  + بعضها يتضمن أدوات مثل "مسجلات النقرات" لجمع كلمات المرور.

**2. البرامج الدعائية:**

* + تعرض إعلانات منبثقة للمستخدم، وقد تجمع بيانات لتوجيه الإعلانات.

**3. برامج الفدية:**

* + تقفل الملفات وتطلب دفع مبلغ مالي لفك التشفير.
  + تنتقل عادة عبر البريد الإلكتروني.

**4. الفيروسات:**

* + تنتشر عبر الشبكات والبريد الإلكتروني.
  + أنواعها تشمل:
    - **الفيروسات المتنقلة**: تنتشر عبر أجهزة متعددة.
    - **فيروس الجذر Rootkit**: يمنح المتسللين سيطرة عن بعد.
    - **حصان طروادة**: يبدو كبرنامج شرعي لكنه يخفي برمجية ضارة.
* **المواقع الإلكترونية غير الموثوقة:**
  + تدفع المستخدم لتنزيل برمجيات خبيثة أو تسحب منه بيانات حساسة.

**🧠 مصطلحات رئيسية مذكورة:**

* **البرامج الضارة**: تهدد البيانات والأنظمة.
* **التشفير**: حماية البيانات من الوصول غير المصرح به.

**✅ تلخيص الصفحة 3 من الملف (صفحة رقم 140):**

**تابع الوحدة 11 – الأمن السيبراني وإدارة الحوادث**

**🔸 القرصنة والتخريب:**

* **القرصنة (Hacking):**
  + محاولة اختراق الأنظمة لأسباب متعددة:
    - التسلية أو الفضول.
    - سرقة أو تدمير البيانات.
    - أهداف تجارية (مثل سرقة تفاصيل منتج).
    - أهداف حكومية (مثل التجسس العسكري أو السياسي).
* **التخريب (Sabotage):**
  + لا يقتصر فقط على سرقة البيانات بل يتضمن **تعطيل الأنظمة**.
  + يتم لأغراض مثل الانتقام، الابتزاز، التنافس التجاري، أو حتى **الإرهاب الإلكتروني**.
  + قد تنفذ الحكومات هجمات لتدمير أنظمة استراتيجية.

**🔸 أمثلة على برامج الفدية الشهيرة:**

1. **CryptoLocker (2013 - 2014):**
   * أصاب 250,000 جهاز.
   * طلب فدية عبر البيتكوين.
2. **WannaCry (2017):**
   * استغل ثغرة في Windows.
   * أصاب حتى أنظمة NHS البريطانية (حوالي 70,000 جهاز).
   * يُعتقد أن مصدره كوريا الشمالية.

**🔸 مصطلحات مهمة:**

* **المتسلل (Hacker)**: من يحاول الدخول إلى الأنظمة بطرق غير مشروعة.
* **هجوم قطع الخدمة (DoS)**:
  + إغراق موقع إلكتروني بطلبات كثيرة ليصبح غير قادر على الاستجابة.
  + النسخة الأكبر منه هي **DDoS** (الموزعة).
  + تهديد خطير لمواقع شركات كبيرة مثل Amazon.

**✅ تلخيص الصفحة 4 من الملف (صفحة رقم 141):**

**تابع الوحدة 11 – الأمن السيبراني وإدارة الحوادث**

**🔸 وقفة للتفكير:**

* **لماذا يحاول الناس اختراق الأنظمة؟**
  + ليس كل المتسللين لديهم نوايا خبيثة.
  + مثال: **القرصان ذو القبعة البيضاء (White Hat Hacker)** يستخدم مهاراته لاكتشاف الثغرات وتحسين الأمان.

**🔸 الهندسة الاجتماعية (Social Engineering):**

* نوع خطير من التهديدات يعتمد على **خداع الأشخاص** داخل المؤسسة.
* مثال: مكالمة هاتفية من شخص يدعي أنه من الدعم التقني يطلب معلومات دخول مثل كلمة المرور.
* يعتمد على "ثقة البشر الطبيعية".

**🔸 تأثير التهديدات السيبرانية:**

1. **خسارة تشغيلية:**
   * الأعطال في الأنظمة تؤدي لتوقف الخدمات أو تراجع الأداء.
   * فيروسات أو هجمات فدية قد تشلّ العمل.
   * الكوارث الطبيعية مثل الحرائق والفيضانات قد تدمر الأجهزة والأنظمة.
2. **التصيد الاحتيالي (Phishing):**
   * نوع من الهندسة الاجتماعية.
   * إنشاء صفحة وهمية لبنك حقيقي وسرقة بيانات الدخول.
   * ينتشر عبر رسائل بريد إلكتروني مزيفة.
   * انخفضت حالات التصيد مؤخرًا بسبب التوعية.

**🧠 أسئلة للتفكير:**

* هل سبق لك أن تعرضت لهجوم تصيد احتيالي؟
* كيف اكتشفت أنه كان تصيدًا؟

**✅ تلخيص الصفحة 5 من الملف (صفحة رقم 142):**

**تابع الوحدة 11 – الأمن السيبراني وإدارة الحوادث**

**🔸 أنواع الخسائر الناتجة عن الهجمات السيبرانية:**

1. **الخسارة المالية:**
   * تحدث عندما تعجز المؤسسة عن تنفيذ عملياتها (بيع، خدمة...).
   * تشمل تكاليف:
     + توظيف خبراء أمن سيبراني.
     + استبدال الأجهزة التالفة أو المسروقة.
     + دفع تعويضات للعملاء (مثل شركات الطيران إذا تأخرت رحلاتها).
     + الغرامات القانونية بسبب تسرب البيانات الشخصية.
2. **خسارة السمعة:**
   * الشركات التي تُخترق قد تفقد ثقة العملاء.
   * العملاء قد يرفضون إدخال بيانات بطاقاتهم مستقبلاً.
   * حتى الموظفون المحتملون قد يترددون في العمل بها.
3. **خسارة الملكية الفكرية:**
   * مثل: أسرار تجارية، أسعار، تصاميم المنتجات.
   * تُسرق في هجمات تهدف إلى كسب ميزة تجارية غير مشروعة.
4. **مستويات التأثير:**
   * تختلف باختلاف حجم الخسائر:
     + مباشرة: مثل سرقة الأموال من حساب الشركة.
     + غير مباشرة: مثل توقف الإنتاج أو الخدمة.

**🔸 تهديدات الأمن السيبراني مع مرور الوقت:**

* تتطور التهديدات باستمرار.
* يجب على المؤسسات تحديث نظم الحماية باستمرار ومواكبة أحدث التهديدات.

**✅ تلخيص الصفحة 6 من الملف (صفحة رقم 143):**

**تابع الوحدة 11 – الأمن السيبراني وإدارة الحوادث**

**🔸 ثغرات النظام:**

1. **ثغرات الشبكة:**
   * المتسللون يستهدفون الشبكات المتصلة بالإنترنت.
   * **جدار الحماية** يُستخدم لحمايتها.
   * **أجهزة USB** المصابة قد تنقل فيروسات إلى الشبكة.
2. **ثغرات تنظيمية:**
   * تحدث بسبب الإعداد السيئ لأنظمة الحاسوب.
   * تشمل:

🔹 **أذونات الملفات والمجلدات:**

* + تُستخدم لتقييد الوصول إلى الملفات على الخوادم.
  + إعدادها بشكل خاطئ قد يؤدي إلى مشاكل في الأمان.

🔹 **الامتيازات:**

* + يجب تقييد صلاحيات المستخدمين (مثلاً منعهم من تثبيت برامج أو تشغيل أوامر خطرة).

🔹 **سياسة كلمات المرور:**

* + من المهم تحديد متطلبات صارمة لكلمات المرور (الطول، التعقيد، التغيير الدوري).
  + كلمات المرور الضعيفة تُعد مدخلاً سهلاً للمتسللين.

1. **ثغرات البرامج:**
   * البرامج غير المرخصة أو القديمة قد تحتوي على برمجيات ضارة.
   * من أكثر الهجمات شيوعًا:

🔸 **حقن SQL**:

* + إدخال أوامر خبيثة في نماذج البحث بمواقع الويب لسرقة البيانات مثل أرقام بطاقات الائتمان.

🔸 **هجمات XSS (البرمجة النصية عبر المواقع)**:

* + يقوم المهاجم بحقن أكواد خبيثة داخل صفحات الويب لسرقة معلومات مثل ملفات تعريف الارتباط.

📌 **مصطلحات مهمة ذكرت:**

* **جدار الحماية (Firewall)**: حاجز أمني بين الشبكة الداخلية والإنترنت.
* **ثغرة أمنية في النظام**: نقطة ضعف يمكن استغلالها للاختراق.
* **SQL و XSS**: تقنيات هجوم تستهدف قواعد البيانات والمواقع الإلكترونية.

**✅ تلخيص الصفحة 7 من الملف (صفحة رقم 144):**

**تابع الوحدة 11 – الأمن السيبراني وإدارة الحوادث**

**🔸 أنواع الثغرات الأمنية:**

1. **ثغرات أمنية غير معروفة (Zero-Day):**
   * تظهر بسبب تأخير تحديث البرامج بعد اكتشاف ثغرة.
   * يستغل المتسللون هذه الفجوة الزمنية قبل إصدار التصحيح.
2. **ثغرات نظام التشغيل:**
   * مثل نظام **Windows XP** الذي لم يعد مدعومًا.
   * التحديثات ضرورية لسد الثغرات، وإلا فإن النظام معرض للاختراق.
3. **ثغرات الأجهزة المحمولة:**
   * تمثل تحديًا لأن الشركات تملك قدرة محدودة على التحكم بها.
   * تعتمد على المستخدم لتحديث النظام، مما يزيد من المخاطر.
   * الأجهزة قد تُفقد أو تُسرق بسهولة.
4. **الثغرات الأمنية المادية:**
   * تتعلق بالمعدات القابلة للسرقة (مثل أجهزة USB أو الحواسيب المحمولة).
   * غالبًا ما تحتوي على بيانات حساسة.
5. **ثغرات عمليات المستخدمين:**
   * **المستخدمون أنفسهم** قد يكونون مصدر خطر:
     + مثل كتابة كلمة المرور على ورقة.
     + أو مشاركة بيانات الدخول مع زملاء آخرين.
6. **ثغرات التقنيات الجديدة:**

🔹 **الحوسبة السحابية (Cloud Computing):**

* + أصبحت شائعة لكن تتطلب الثقة بمزود الخدمة.
  + الأمان يعتمد على الشركة المزودة وليس فقط المستخدم.

🔹 **إنترنت الأشياء (IoT):**

* + مثل الكاميرات الذكية وأجهزة التتبع.
  + عند اختراقها، يمكن معرفة أوقات غيابك أو حتى التحكم في الأنظمة عن بعد.

📌 **مصطلح مهم:**

* **إنترنت الأشياء (IoT):** شبكة من الأجهزة المتصلة بالإنترنت (مثل الكاميرات، الثلاجات، أجهزة التكييف...).

**✅ تلخيص الصفحة 8 من الملف (صفحة رقم 145):**

**تابع الوحدة 11 – الأمن السيبراني وإدارة الحوادث**

**🔸 المسؤوليات القانونية وموضوعات الأمان:**

1. **نواقل الهجوم (Attack Vectors):**
   * الطرق التي يستخدمها المتسللون للوصول إلى الأنظمة.
   * من أمثلتها: **Wi-Fi، Bluetooth، الإنترنت، أو الشبكة الداخلية (LAN)**.
2. **حماية البيانات (Data Protection):**
   * **اللائحة العامة لحماية البيانات (GDPR)** في أوروبا تُنظم كيفية جمع ومعالجة البيانات الشخصية.
   * أهم مبادئها:
     + معالجة قانونية.
     + جمع البيانات لغرض محدد فقط.
     + تقليل البيانات للمطلوب فقط.
     + الاحتفاظ بها للفترة اللازمة فقط.
     + ضمان أمن البيانات.
   * تعطي الأفراد حقوقًا، منها:
     + الحق في معرفة متى تُجمع بياناتهم.
     + الوصول لبياناتهم.
     + طلب حذفها.
     + الاعتراض على استخدامها.
3. **تشريعات إساءة استخدام الحاسوب (Computer Misuse Law):**
   * مثل القانون البريطاني لعام 1990، الذي يُجرم:
     + الدخول غير المصرح به.
     + التخريب.
     + استخدام أدوات إلكترونية للقرصنة.
4. **تشريعات الاتصالات:**
   * يحق لأرباب العمل مراقبة البريد الإلكتروني والاتصالات في شبكاتهم بشرط أن يكون الموظفون على علم بذلك (مثلاً عبر عقد العمل).

📌 **مصطلحات مهمة:**

* **GDPR:** قانون لحماية البيانات الشخصية في أوروبا.
* **LAN:** شبكة محلية داخل مؤسسة.
* **هجوم يوم الصفر (Zero-Day):** استغلال ثغرة لم تُعالج بعد.

**✅ تلخيص الصفحة 9 من الملف (صفحة رقم 146):**

**تابع الوحدة 11 – الأمن السيبراني وإدارة الحوادث**

**🔸 تشريعات إضافية وتدابير الأمان:**

1. **تشريعات مكافحة الاحتيال:**
   * تشمل الهجمات التي تُنفذ بهدف **الحصول على أموال بطرق غير قانونية**.
   * مثل استخدام بيانات مسروقة (الاسم، العنوان، رقم الحساب البنكي) للتقديم على قروض بنكية.
2. **الصحة والسلامة:**
   * تفرض القوانين على المؤسسات حماية الموظفين في بيئة العمل.
   * وتشمل أيضًا مسؤوليات على الموظفين بعدم تعريض الآخرين للخطر.
3. **تدابير الأمان المادي (Physical Security):**
   * لحماية الأجهزة والبيانات من السرقة أو الوصول غير المصرح به، مثل:
     + **أقفال الأبواب وغرف الخوادم.**
     + استخدام **بطاقات أو كلمات مرور** للتحكم بالدخول.
     + **إخفاء الكوابل** وأجهزة الشبكة لحمايتها.
     + استخدام أنظمة **CCTV (الكاميرات)** للتسجيل والمراقبة.
     + **أفراد أمن** لتفتيش الزوار.
     + **أجهزة إنذار** لاكتشاف الدخول غير المصرح به.
4. **دراسة حالة حقيقية:**
   * في 2014، تم اتهام مواطن بريطاني يعاني من **متلازمة أسبرجر** باختراق أنظمة حساسة في الولايات المتحدة مثل:
     + مكتب التحقيقات الفيدرالي (FBI)
     + الجيش الأمريكي
     + وكالة الدفاع الصاروخي
   * لم تتم محاكمته في أمريكا بسبب ظروفه الصحية.

📌 **فكرة أساسية:**

الأمان المادي لا يقل أهمية عن الأمان البرمجي. الأجهزة التي تحتوي على معلومات حساسة يجب تأمينها فعليًا.