المركز الوطني
للأمن السيبراني
National Cyber
Security Center

الأمن المادي

المحـــــاور

- الأمن المادي في سياق الأمن السيبراني
- تعريف الأمن المادي
- أهمية تحقيق الأمن المادي
- تهديدات الأمن المادي
- إجراءات تحقيق الأمن المادي

الأمن المادي في سياق الأمن السيبراني

يُعنى مفهوم الأمن السيبراني بحماية المؤسسات والأشخاص والبنى التحتية والأنظمة والشبكات والأجهزة من أي تهديد أو خطر ومنع الوصول غير المرخص إلى المعلومات والبيانات؛ فكما يتم حماية الأنظمة البرمجية والشبكات والمواقع من الثغرات التقنية وكما يتم إجراء العديد من إجراءات الأمان عبر الإنترنت فإن الأمن السيبراني يُعنى أيضاً بحماية تلك البيانات والمعلومات والأنظمة والأجهزة وحتى المباني وغيرها حماية مادية واتخاذ الإجراءات والتدابير التي تضمن عدم تعرضها للتخريب أو الوصول غير المصرح به من قبل أيٍ كان.

تعريف الأمن المادي

يُشير مفهوم الأمن المادي إلى مجموعة السياسات والإجراءات والتدابير التي تهدف إلى حماية الممتلكات الفعلية والموارد المادية التي يتم استخدامها ضمن أنظمة تكنولوجيا المعلومات، فالأمن المادي يُركز على حماية الأجهزة والبنية التحتية الأساسية.

أهمية تحقيق الأمن المادي

إن تحقيق الأمن المادي للأجهزة والمعدات التقنية المختلفة أمر بالغ الأهمية في تحقيق الأمن السيبراني للأفراد والمؤسسات، حيث يتعلق هذا الامر بالحفاظ على البيانات والمعلومات وهو ما ينعكس بدوره على حماية أصول المؤسسات وضمان استمرار تقديم الخدمات بالشكل المطلوب.

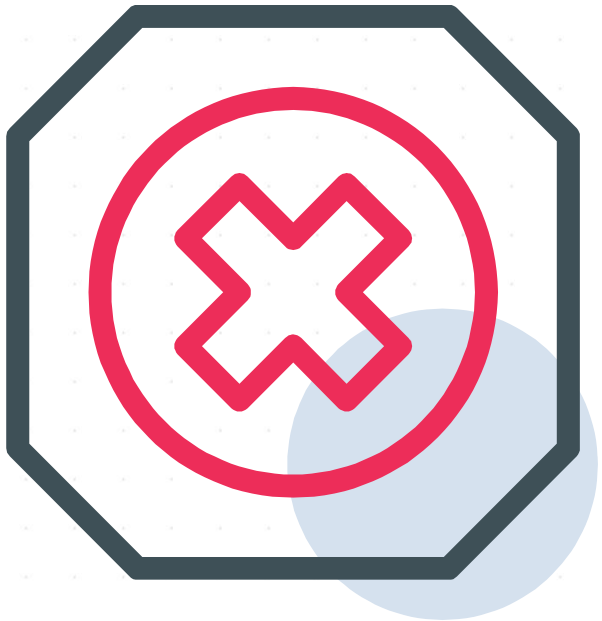
تهديدات الأمن المادي

تُشكل تهديدات الأمن المادي تحديات كبيرة في مجال الأمن السيبراني، فالأثر الذي قد يترتب عن تلك التهديدات لا يقل خطراً وأهمية عن التحديات التي تخلقها الجرائم السيبرانية التي يتم شنها إلكترونياً وعبر الإنترنت، وفيما يأتي بعض أهم تهديدات الأمن المادي:

تهديدات الأمن المادي

السرقة الفيزيائية: حيث تمتلك جميع المؤسسات والدوائر مستندات ووثائق أو حتى أجهزة أو أقراص تخزين أو غيرها من أنواع الأصول القيّمة التي قد يتم سرقتها والاستيلاء عليها من قبل اللصوص.

تهديدات الأمن المادي

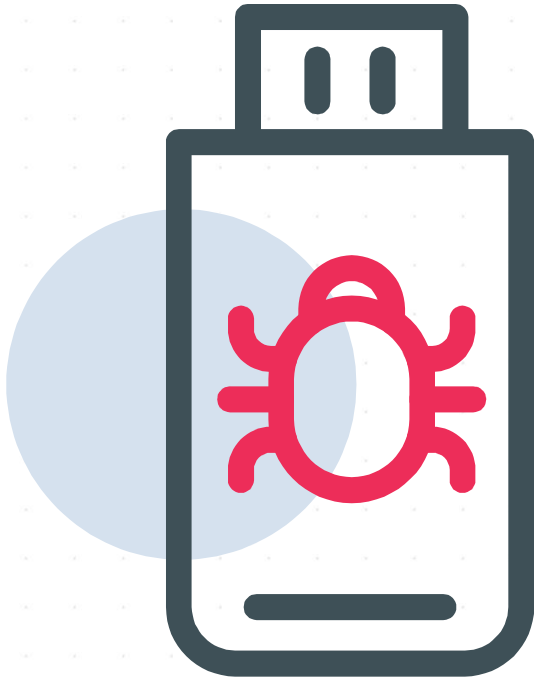


الدخول غير المصرح: ويقصد به أن يتم الدخول إلى أي موقع ومكان من قبل أشخاص غير مخول لهم ولا يحق لهم التواجد في ذلك المكان، ويُمكن أن يحدث مثل هذا التهديد بواسطة طرق مختلفة، كالدخول خلسة أو الدخول بواسطة بطاقة دخول مزورة أو غيرها من الطرق.

تهديدات الأمن المادي

التجسس: لا ينحصر خطر التجسس على الاختراق عبر الإنترنت، حيث يُمكن أن يقوم أحدهم بالتجسس على أعمال الموظف أو المؤسسة بشكل فيزيائي، من خلال المراقبة أو غيرها من أشكال التجسس.

تهديدات الأمن المادي



التخريب: من التهديدات الأمنية للمؤسسات حدوث تخريب لأي من البنى التحتية والأجهزة التي يُمكن أن تُعيق عمل المؤسسة، كقطع أسلاك الاتصال على سبيل المثال، وغيرها من أنواع التخريب الأخرى.

تهديدات الأمن المادي

الهندسة الاجتماعية: تأتي هجمات الهندسة الاجتماعية في مجموعة كبيرة ومتنوعة من الأشكال المختلفة، مما يجعل مكافحتها أمراً بالغ الصعوبة، وتعتمد هجمات الهندسة الاجتماعية على مبدأ التلاعب بالأشخاص أو الموظفين باستخدام المعلومات التي تمكنهم من انتحال شخصية شخص آخر وإساءة استخدام التعاطف البشري للوصول إلى معلومات وشبكات آمنة، فعلى سبيل المثال؛ أحد أكثر هجمات الهندسة الاجتماعية شيوعا ما يُعرف بـ "حيلة القهوة"؛ حيث يقوم شخص ما بحمل فنجاني قهوة واحد في كل يد ويسير باتجاه باب المكتب مما يجعل الموظف القريب أو المار بجوار المكتب القيام بفتح الباب من باب المجاملة، و بالتالي السماح لشخص غير مصرح له بدخول المكتب.

إجراءات تحقيق الأمن المادي

- **فيما يأتي بعض أهم الإجراءات التي يُمكن اتباعها لتحقيق الأمن المادي للمؤسسة:**
- **تأمين البنية التحتية والمرافق:** وذلك من خلال وضع أنظمة مراقبة وإنذار على المباني والمناطق وخاصة الحرجة منها والهامة، كما يُوصى بتركيب أنظمة قفل بيو مترية كأنظمة البصمة أو أنظمة التعرف على الوجه وغيرها مما يُعزز أمن المنشأة ويحد من خطر دخول الغرباء أو غير المصرح لهم.

إجراءات تحقيق الأمن المادي

- **حماية الأجهزة المحمولة والمتنقلة:** يشتمل الأمن المادي الحفاظ على الأجهزة المحمولة كأجهزة اللابتوب والهواتف الذكية والأجهزة اللوحية وتأمينها ضد خطر التعرض للتجسس أو السرقة أو غيرها مما قد يضر بسلامة المؤسسة أو الفرد المالك لهذه الأجهزة، سواء من خلال تشفير بيانات تلك الأجهزة او تطبيق السياسات الصحيحة لإدارة الأجهزة المحمولة وتفعيل بروتوكولات الحماية من السرقة والفقدان.

إجراءات تحقيق الأمن المادي

- **حماية وسائل التخزين:** ويتضمن ذلك توفير مكان آمن لتخزين البيانات الحساسة بالإضافة إلى تشفير البيانات الهامة عند تخزينها أو نقلها، وذلك لزيادة درجة الحماية المادية لهذه البيانات، ويتضمن هذا الإجراء تلك الأجهزة التي يتم تخزين البيانات عليها كالأقراص الصلبة أو حتى خوادم التخزين.

إجراءات تحقيق الأمن المادي

- **إدارة وصول الأشخاص:** لتحقيق الأمن المادي فإنه لا بد من تقييد وصول الأشخاص سواء الموظفين أو حتى الزوار للمواقع والمكاتب المختلفة داخل المؤسسة أو الدائرة، حيث يتوجب أن يكون هناك سياسة دخول توضح الأماكن التي يحق لكل موظف التواجد فيها وبما لا يُعرض أي من بيانات أو مصادر المؤسسة للانتهاك أو التجسس أو غيرها من المخاطر، كما يتوجب أن يتم تفعيل هذه السياسات من خلال شارات دخول مغناطيسية ذات صلاحيات محددة لكل موظف.

إجراءات تحقيق الأمن المادي

- **سياسة المكتب النظيف:** وهي توجيه مؤسسي يحدد كيف يجب على الموظفين ترك مساحة عملهم عند مغادرة المكتب، وتهدف سياسة المكتب النظيف إلى ضمان تنظيف مساحات العمل، وإغلاق المستندات الحساسة أو حفظها بشكل مناسب في نظام الكمبيوتر.، وتعد سياسة المكتب النظيف بمثابة تذكير يومي للموظفين بأن حماية المعلومات والبيانات السرية تمثل أولوية قصوى للحماية من الانتهاكات الأمنية.

إجراءات تحقيق الأمن المادي

تطبيق سياسة المكتب النظيف: وذلك من خلال الآتي:

- يجب أن يكون جهاز الكمبيوتر الخاص بك محميا بكلمة مرور.
- يجب تفعيل قفل أمان لجهازك بعد ثلاث دقائق من تركه كحد أقصى.
- يجب أن يكون قفل أمان جهازك محميا بكلمة مرور أو يتطلب منك التحقق من بصمة الإصبع لإعادة فتحه.
- أغلق أجهزتك عندما تغادر المكتب في نهاية اليوم.
- لا ينبغي تعيين شاشة التوقف لأجهزة الكمبيوتر (المكتبية أو المحمولة).
- يجب تخزين الورق ووسائط الكمبيوتر في خزائن مقفلة مناسبة عندما لا تكون قيد الاستخدام.

إجراءات تحقيق الأمن المادي

تطبيق سياسة المكتب النظيف: وذلك من خلال الآتي:

- يجب مسح المعلومات الحساسة من الطابعات فور طباعتها.
- يجب أن يظل مكتب الاستقبال خاليا قدر الإمكان في جميع الأوقات.
- يجب حفظ المتعلقات الشخصية الفردية في أدراج مقفلة.
- تأكد من عدم ترك أي أوراق أو متعلقات على المكتب قبل المغادرة نهاية اليوم.
- يجب أن تحتوي أجهزة سطح المكتب على اختصارات فقط وأن لا تحتوي على ملفات أو مجلدات كاملة.
- يجب أن تكون شاشات الكمبيوتر بزاوية بعيدة عن أنظار الأشخاص غير المصرح لهم في الغرفة. يجب أن تظل غرف الخادم / مناطق المكاتب مغلقة عندما لا تكون قيد الاستخدام.
- يجب تأمين خزائن الملفات في حالة عدم استخدامها.
- يجب عدم نشر كلمات المرور في أي مكان يمكن الوصول إليه.
- يجب إزالة نسخ المستندات التي تحتوي على معلومات سرية على الفور.

الخاتمة

إن تحقيق الأمان المادي والفيزيائي للأجهزة والمعدات التقنية وحتى الوثائق المطبوعة هو جزء لا يتجزأ من تحقيق الأمن السيبراني والوصول إلى الحماية الرقمية الفعالة، ولكن هذا لا يُلغي أهمية الأمان الرقمي الذي يهتم بحماية البرمجيات وسد الثغرات التقنية والفنية في الأنظمة والأجهزة والشبكات، فالتوازن الجيد بين كل من الأمان المادي والأمان التقني يقود إلى توفير حماية شاملة للأنظمة والمعلومات والبيانات.

نتمنى لكم السلامة في

العالم

الرقمي.