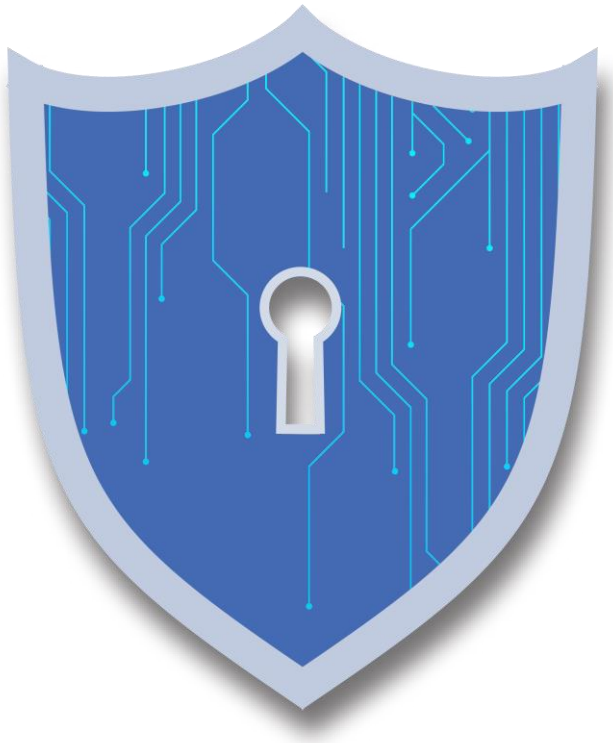
سياسة أمن الأنترنت

السياسات العامة لأمن المعلومات

في الجهات الحكومية

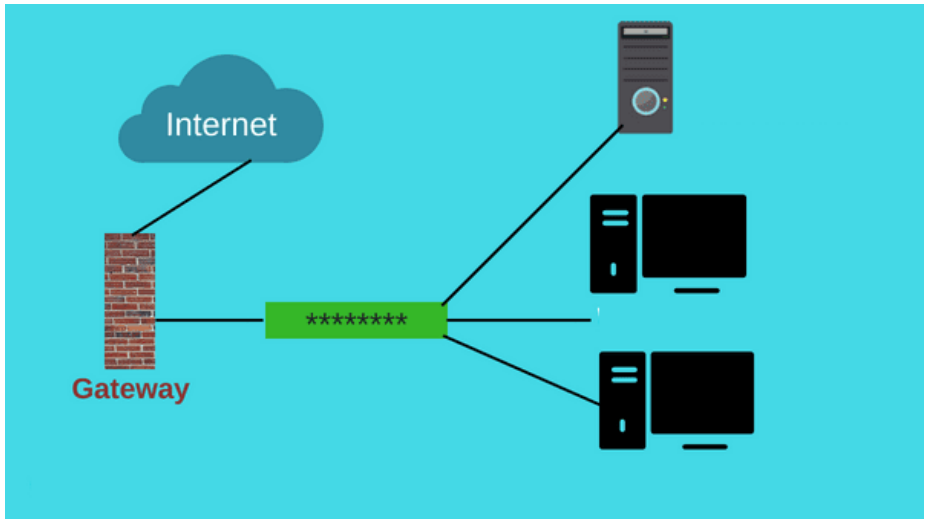
م / محمد الجائفي

المحاور



- بنود سياسة أمن الإنترنت
- المقدمة
- الاهداف
- النطاق
- من أهم الحلول والتكنولوجيا الأمنية للإنترنت
- الأدوار والمسئوليات

بنود سياسة أمن الإنترنت



يجب أن تكون جميع طرق الوصول إلى الإنترنت إما عن طريق مركزية لبوابات الإنترنت أو من خلال بوابة الإنترنت الخاصة بالجهة بما يتماشى مع المعايير الأمنية

على الجهات الحكومية أن تنظر في الفائدة من حجب بعض المواقع غير الخاصة بالعمل مثل مواقع التواصل الاجتماعي، مع الأخذ بعين الاعتبار أن عدم فلترة بعض المواقع لا يعني السماح للموظف بتصفح تلك المواقع

بنود سياسة أمن الإنترنت

يجب أن يوضح كل قسم أو إدارة للمستخدمين لديه سياسته فيما يتعلق بالاستخدام المقبول للإنترنت

لا يجوز للموظفين تنصيب أي برامج تم تحميلها من شبكة الإنترنت ما لم يكن من مصدر موثوق بها وبعد موافقة إدارة/ قسم/مختص أمن المعلومات بالجهة

بنود سياسة أمن الإنترنت

يجب أن تحدد الجهة الحكومية سياستها بوضوح تجاه استخدام خدمات الإنترنت المجانية/التجارية لأداء الأعمال الحكومية سواءً الخدمات الممنوحة للأفراد أو المؤسسات مثل خدمات البريد الإلكتروني العامة مثل (Gmail, mail,...etc.) وخدمات وسائل التواصل الاجتماعي مثل (واتساب, تيلجرام,...الخ) وخدمات التخزين السحابية للملفات مثل (google Drive, Dropbox) فيما يخص أعمال الجهة وإرسال واستقبال الوثائق ونحوها

بنود سياسة أمن الإنترنت

يمنع على الجهة الحكومية تخزين وحفظ بيانات الجهة الحكومية أو معلوماتها أو أنظمتها على منصات الحوسبة السحابية خارج الوطن ويجب أن تكون مخزنة على منصات تلك الجهة داخلياً أو لدى مزود خدمات المعطيات الوطني

يجب أن تكون مو اقع الإنترنت الخاصة بالجهات الحكومية مستضافة داخل البلد ويمنع استضافتها في الخارج

سياسة أمن الإنترنت- مقدمة

يتعرض الإنترنت لمجموعة متنوعة من التهديدات التي تشمل الاختراقات السيبرانية، والفيروسات، وبرامج التجسس، والاحتيال الإلكتروني، والتطفل على الخصوصية، وغيرها. تهدف هذه التهديدات إلى الوصول غير المصرح به إلى المعلومات الحساسة، وسرقة البيانات خاصة الحكومية والرسمية، وتعطيل الأنظمة. ويعتبر أمن الإنترنت هو المجال الذي يهتم بحماية الأنظمة والشبكات والبيانات والمعلومات التي تمتلك اتصال بشبكة الإنترنت من التهديدات السيبرانية

لتأمين وحماية المعلومات والتجهيزات من تهديدات الاتصال بشبكة الانترنت، يجب على الجهة وضع سياسة خاصة بأمن الإنترنت توضح فيها الضوابط والتعليمات المناسبة والاستخدام المقبول للإنترنت وعمل الإجراءات اللازمة لتأمين وحماية التجهيزات والخدمات المتصلة بالإنترنت من أي محاولات اختراق بما يتوافق مع سياسات أمن المعلومات

كما يمكن تعريف سياسة أمن الإنترنت بمجموعة من الإرشادات والإجراءات التي تنفذها الجهة لحماية أنظمتها والشبكات والبيانات الخاصة بها من الوصول غير المصرح به وسوء الاستخدام والتهديدات المحتملة عبر استخدام الانترنت. تحدد هذه السياسة القواعد والمسؤوليات للموظفين والمستخدمين فيما يتعلق باستخدام الإنترنت والموارد الرقمية داخل الجهة.

تعتمد سياسة أمن الإنترنت على مجموعة من المبادئ والممارسات التقنية والسلوكية للحفاظ على سلامة وسرية المعلومات والبيانات والحماية من الهجمات السيبرانية

الأهداف

تهدف هذه السياسة الى:

تحديد ووضع التعليمات والضوابط الأساسية واللازمة لأمان شبكة الإنترنت والاستخدام المقبول للإنترنت والإجراءات اللازمة لحماية الجهة الحكومية وكل ما تمتلكه من موارد معلوماتية وتجهيزات من أي عمليات اختراق ووصول عبر الإنترنت.

حماية وتأمين البيانات والمعلومات الحكومية المتصلة بالإنترنت من الوصول غير المصرح به. يتم تطبيق تقنيات الحماية والتشفير وآليات التحقق من الهوية وسياسات الوصول المناسبة لضمان سرية وسلامة البيانات

حماية البنية التحتية الرقمية للجهة الحكومية، بما في ذلك الشبكات والأجهزة والأنظمة من خلال تطبيق تدابير الأمان اللازمة لعزل ومنع واكتشاف واستجابة للتهديدات السيبرانية مثل الاختراقات والفيروسات والهجمات الإلكترونية الأخرى

تعزيز الوعي والتدريب للموظفين والمستخدمين بشأن مخاطر الأمان السيبراني وأفضل الممارسات الأمنية. يتم توفير برامج تدريبية وحملات توعية لتعريف الموظفين بالتهديدات السيبرانية وكيفية التعامل معها واتباع إجراءات الأمان اللازمة

النطاق

تسري هذه السياسة على الجهات الحكومية التي تمتلك وتستخدم شبكة الإنترنت لأداء الاعمال الحكومية وتطبق على كافة مكونات شبكة الأنترنت والأجهزة المتصلة بها بشكل مباشر او غير مباشر، وعلى كافة العاملين والمستخدمين المتصلة أجهزتهم بالإنترنت

من أبرز التهديدات الأمنية لاستخدام الإنترنت

تهديدات خارجية (EXTERNAL THREATS)

- Port Redirection
- Network Spoofing
- Man-in-Middle
- Hacker / Cracker
- Worms
- Adware

- Viruses
- Spams
- Phishing
- Malware
- Trojan Horse
- Social Engineering
- Malicious Spyware

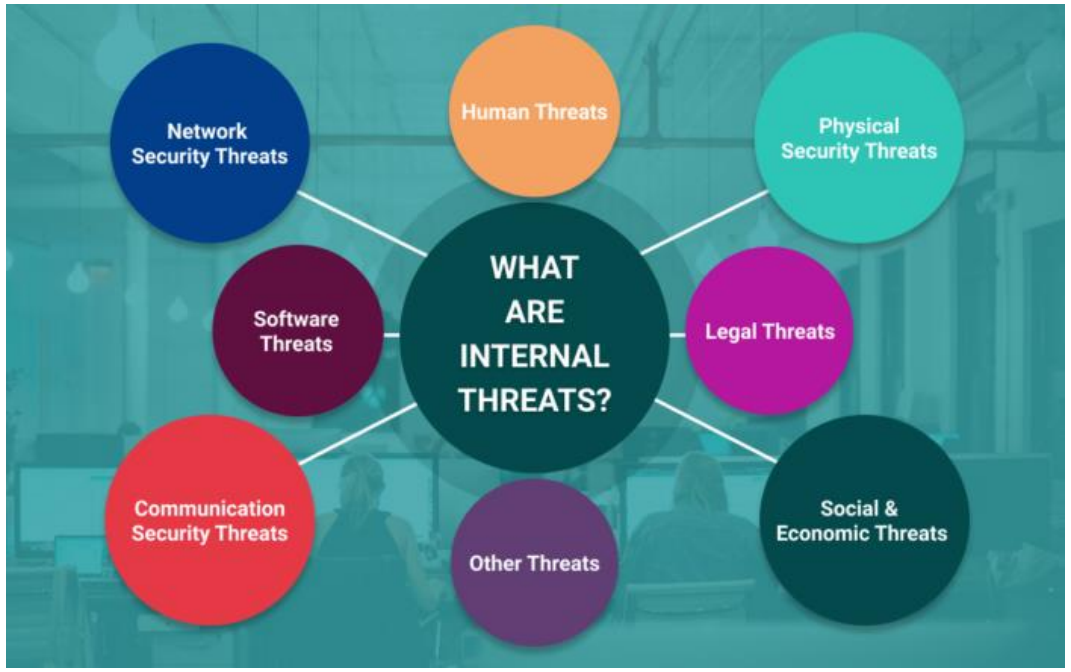
تهديدات داخلية (INTERNAL THREATS)

- سوء استخدام الموظفين (Employee Abuse)
- اعطال وفشل تشغيلي (Operational/System Failures)
- نقاط ضعف في الأنظمة (System Vulnerabilities)
- إدارة ضعيفة لكلمات المرور(Poor password management)
- إساءة استخدام الصلاحيات: يحدث هذا عندما يسيء مستخدم مرخص له يتمتع بإمكانية وصول مرتفعة استخدام امتيازاته لإيذاء الجهة
- السلوك المهمل: تجاهل الموظفين للسياسات الأمنية وينخرطون في سلوك محفوف بالمخاطر يمكن أن يؤدي إلى خرق البيانات. على سبيل المثال، قد يستخدم أحد الموظفين شبكة Wi-Fi عامة غير آمنة للوصول إلى بيانات الجهة عبر الانترنت

من أبرز التهديدات الأمنية لاستخدام الإنترنت

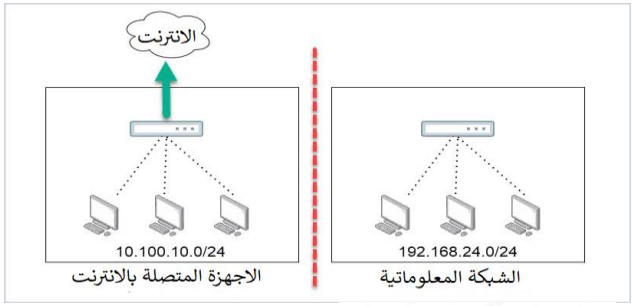
تهديدات خارجية (EXTERNAL THREATS)

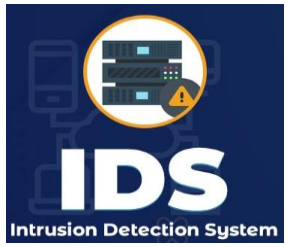
تهديدات داخلية (INTERNAL THREATS)

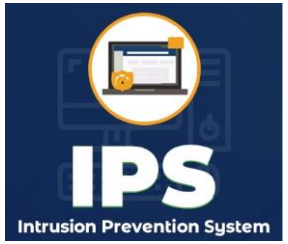


من أهم الحلول والتكنولوجيا الأمنية عند استخدام الإنترنت

- إعداد سياسة توضح التعليمات والاجراءات والضوابط اللازم تطبيقها لحماية تجهيزات وشبكات و أنظمة الجهة الحكومية عند استخدام الإنترنت او الوصول له او ربطه بالتجهيزات، بالإضافة الى تحديد الاستخدام المقبول للإنترنت.
- عزل الأجهزة المتصلة بالأنترنت بشبكة منفصلة ومستقلة مادياً عن الشبكة المعلوماتية الخاصة بالجهة (Physical Isolation)
- أجهزة جدار الحماية (Firewall)
- Encryption / Authorization
- أجهزة (IPS / IDS)
- جدار حماية تطبيقات الويب والتصفية (WAF / Web Filtering)
- استخدم برامج الحماية من الشفرات الخبيثة مثل (Anti-virus, anti-spam, anti-spyware, etc.)
- Internet Protocol Security (IPsec) / Secure Socket Layer (SSL)







الأدوار والمسئوليات

تحديد الأدوار والمسئوليات لكل من:

- الجهة الحكومية (قيادة الجهة الحكومية)
- مدير النظام ومسئول الشبكة
- ضابط أمن المعلومات
- المستخدمين

انتهى،،،