المركز الوطني
للأمن السيبراني
National Cyber
Security Center

التشفير

المحـــــاور

- مقدمة في التشفير
- تعريف التشفير
- آلية عمل التشفير
- أنواع التشفير
- ضوابط التشفير
- أفضل الممارسات العامة في التشفير
- الخاتمة

مقدمة في التشفير

في ظل التقدم السريع للتكنولوجيا وتزايد التواصل الإلكتروني واعتماد المؤسسات والأفراد على الخدمات الإلكترونية عبر الإنترنت أصبحت الحاجة ملحة لضمان أمن المعلومات والبيانات التي تنتقل عبر أنواع الشبكات المختلفة سواء تلك الداخلية أو حتى عبر شبكة الإنترنت العالمية، ويأتي ذلك مع اتساع رقعة التهديدات السيبرانية المختلفة وامتلاك مجرمي الإنترنت والقراصنة لمهارات وأدوات فنية تُسهل عليهم الوصول إلى شتى أنواع البيانات والمعلومات والتجسس عليها، ومن هنا يظهر ما يُعرف بمفهوم التشفير الذي يُعد جزءاً رئيسياً وحيوياً من استراتيجيات تحقيق الأمن السيبراني.

تعريف التشفير

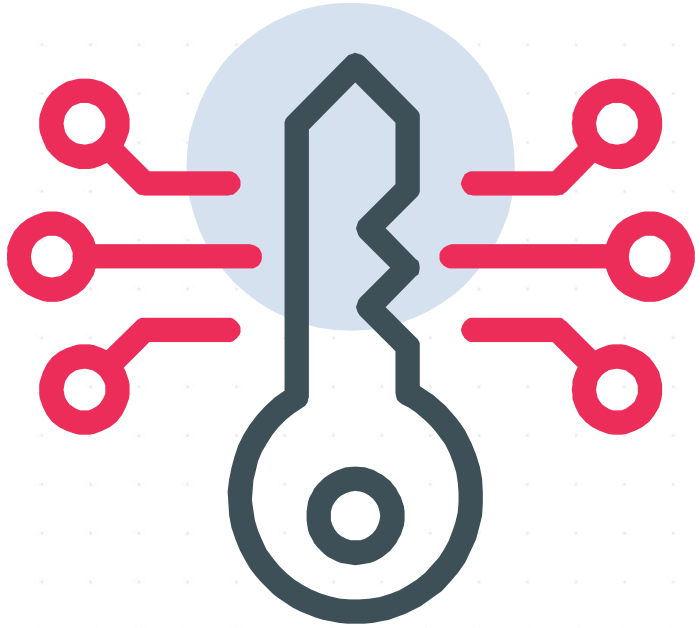
- يُشير مفهوم التشفير في الأمن السيبراني إلى عملية تحويل المعلومات من نص مفهوم وقابل للقراءة إلى نص غير مفهوم، يتطلب فك التشفير لقراءته مرة أخرى.
- يحول التشفير البيانات إلى شكل غير مقروء باستخدام خوارزميات رياضية مُعينة.
- يُستخدم التشفير في حماية بيانات الاتصالات عبر الإنترنت والرسائل الإلكترونية والمعلومات الحساسة في الأنظمة والأجهزة، بما في ذلك الحواسيب والهواتف المحمولة.

آلية عمل التشفير

يُمكن تلخيص مبدأ عمل آلية التشفير كالتالي:

- البيانات المُراد تشفيرها: عادة تكون نصوص حساسة يرغب المستخدم في حمايتها لضمان عدم الاطلاع غير المصرح عليه.
- اختيار طريقة التشفير: هناك العديد من آليات وطرق التشفير التي تستخدم لتحويل البيانات إلى أشكال غير قابلة للقراءة، و يجب اختيار خوارزمية التشفير المناسبة لتحديد كيفية تحويل البيانات من شكلها الأصلي إلى شكل غير واضح.

آلية عمل التشفير



- مفتاح التشفير: هو مجموعة من البيانات (أرقام أو حروف) تُستخدم لاستعادة البيانات المشفرة إلى شكلها الأصلي، ويتم إنشاء مفتاح فك التشفير أثناء عملية التشفير باستخدام خوارزميات التشفير، ويكون ضروريًا لأي طرف يرغب في فك تشفير البيانات واستعادتها إلى حالتها الأصلية.
- عملية التشفير: وهي العملية التي تقوم خلالها برامج التشفير المختلفة بتحويل النص الأصلي إلى شكل غير مفهوم باستخدام أحد خوارزميات التشفير المتوفرة في تلك البرامج.

آلية عمل التشفير

- البيانات المُشفرة: هي معلومات التي تم تحويلها إلى شكل غير قابل للقراءة باستخدام تقنيات التشفير، و المتطلبة لمفتاح فك التشفير لاستعادتها إلى شكلها الأصلي.
- تخزين البيانات أو النقل: حيث يُمكن تخزين البيانات المُشفرة أو نقلها دون الاكتراث والخوف من الاطلاع والوصول غير المُصرح.
- فك التشفير: وهي العملية التي يتم خلالها إعادة البيانات من شكلها المُشفر وغير الواضح إلى حالتها الأصلية وذلك باستخدام مفتاح فك التشفير.

أنواع التشفير

يوجد العديد من أشكال وأنواع التشفير والتي تختلف باختلاف الاستخدامات ومتطلبات الأمان، ولكن يُمكن تصنيف أنواع التشفير الأكثر شيوعاً واستخداماً تبعاً لنوع مفتاح التشفير الذي يتم استخدامه؛ وما إذا كان يتم استخدام المفتاح نفسه للتشفير ثم لفك التشفير أم لا؛ كالآتي:

أنواع التشفير

التشفير المُتماثل

يستخدم نفس المفتاح لكل من عملية التشفير وفك التشفير.
يعرف أيضاً بتشفير المفتاح الواحد، حيث يتم استخدام مفتاح واحد لكل من تشفير وفك تشفير البيانات.

التشفير غير المُتماثل

يتم في هذه الطريقة من التشفير استخدام مفتاحي تشفير مختلفين لدى كل من مُرسل البيانات ومُستقبلها، أحدهما خاص والآخر عام ومرُتبطين ببعضهما البعض حسابياً، ولكنهما ليسا متشابهين ومتماثلين.
يحتفظ الطرف المُرسل بالمفتاح الخاص بشكل سري وحصري له، بينما يكون المفتاح العام مُشاركاً بين المُستلِمين المُصرح لهم أو حتي يُمكن إتاحته للجمهور بشكل عام، ولا يُمكن فك تشفير البيانات المُشفرة من خلال المفتاح الخاص إلا باستخدام المفتاح الخاص المُقابل.

ضوابط التشفير

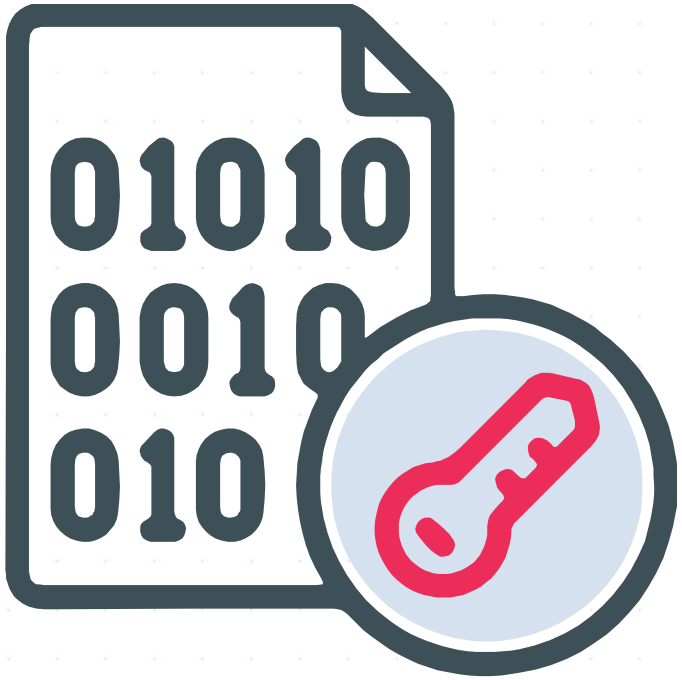
لضمان فعالية تحقيق الحماية السيبرانية للبيانات والتأكد من سلامتها فإنه لا بد أن تتماشى عمليات التشفير التي تحدث في أي مؤسسة مع مجموعة من الضوابط الأساسية، والتي منها الآتي:

- **اختيار طرق تشفير قوية:** وذلك من خلال اختيار خوارزمية تشفير قوية و موثوقة وقابلة للتحديث بشكل مُستمر لتتماشى مع التصدي للهجمات الرقمية الحديثة.
- **إدارة مفاتيح التشفير:** تُعتبر مفاتيح التشفير العامل الرئيسي في عملية التشفير بأكملها لذا فإنه يتوجب أن يتم تأمين إدارة هذه المفاتيح بشكل جيد لحمايتها من الاطلاع والتجسس.

ضوابط التشفير

- **السرعة:** يجب أن تكون عملية تشفير البيانات سريعة وفعالة لتلبية متطلبات الأداء، وبشكل خاص عند تشفير كميات كبيرة من البيانات والمعلومات.
- **تفعيل أنظمة المصادقة:** لا بد أن يُرافق عملية التشفير تفعيل أنظمة المصادقة المتعددة التي تقوم على مبدأ استخدام طبقات متعددة من الأمان وذلك لتعزيز منظومة الأمن السيبراني كاملة.
- **التوقيع الرقمي:** لضمان التحقق من صحة البيانات المُشفرة التي يتم تبادلها وللتحقُق من هوية الأطراف المُرسلة والمُستقبلة لتلك البيانات فإنه لا بد أن يتم استخدام التوقيع الرقمي من كلا الطرفين.

أفضل الممارسات العامة في التشفير



يوجد العديد من الممارسات التي يتوجب اتباعها لإدارة عملية التشفير بشكل فعال وناجح ومن هذه الممارسات الآتي:

- التأكد من تشفير البيانات أثناء النقل و التخزين بناءً على تصنيفها و حسب السياسات و الإجراءات التنظيمية للمؤسسة و المتطلبات التشريعية والتنظيمية ذات العلاقة.

- استخدام طرق وخوارزميات ومفاتيح وأجهزة تشفير محدثة وفقاً لنظام الأمن السيبراني أو تكنولوجيا المعلومات المُتبع في المؤسسة.

أفضل الممارسات العامة في التشفير

- تشفير جميع بيانات الأنظمة الحساسة أثناء النقل أو التخزين على مستوى الملفات و قواعد البيانات أو على مستوى أعمدة محددة داخل قواعد البيانات.
- تطبيق التشفير وفقاً لحلول التشفير المعتمدة والمتوفرة على مستوى المؤسسة.
- استخدام طرق التحقق الآمن مثل استخدام مفاتيح التشفير العامة و التواقيع الرقمية و الشهادات الرقمية للحد من المخاطر السيبرانية ووفقاً لحلول التشفير المعتمدة في المؤسسة.

أفضل الممارسات العامة في التشفير

- إستخدام التحقق من هوية المستخدم لنقل البيانات السرية للغاية إلى أطراف خارجية باستخدام شهادات التشفير الرقمية المعتمدة و وفقاً لسياسة حماية البيانات و المعلومات المعتمدة في المؤسسة.
- إصدار شهادات التشفير عن طريق جهة موثوقة ومُعتمدة لدى المؤسسة.
- حفظ معلومات المفاتيح الخاصة في مكان آمن و الحرص على منع الوصول غير المصرح لها وتوفير التقنيات اللازمة لحفظ مفاتيح التشفير عند تخزينها.

أفضل الممارسات العامة في التشفير

- تصنيف مفاتيح التشفير الخاصة باعتبارها معلومات سرية للغاية وفقاً لسياسة تصنيف البيانات المعتمدة في المؤسسة.
- تحديد مدة صلاحية لاستخدام مفاتيح التشفير وتوثيق تاريخ الإنشاء وتاريخ الانتهاء لكل مفتاح.
- تجديد مفاتيح التشفير قبل انتهاء صلاحيتها.
- توفير قنوات بديلة لنقل مفاتيح التشفير خلالها في حال تعذُر إمكانية تبادل المفاتيح بين كل من المرسل والمستقبل بشكل آمن وموثوق.

الخاتمة

في ظل تزايد مستمر للهجمات والتهديدات السيبرانية المختلفة يظهر التشفير كسلاح فعال في مجال حماية المعلومات وتأمينها، لذا فإنه يتوجب على المؤسسات المختلفة تكثيف جهودها في تطوير واعتماد طرق تشفير قوية لضمان سرية معلوماتها ومعلومات عملاءها.

نتمنى لكم السلامة في

العالم

الرقمي.