حماية البيانات السرية

الفئة المستهدَفة
منظمات المجتمع المدني

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

حماية البيانات السرية

الفئة المستهدَفة: منظمات المجتمع المدني

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

حقوق الملكية الفكرية

المادة مملوكة للوكالة الوطنية للأمن السيبراني في دولة قطر، وكافة حقوق الملكية الفكرية التي تشمل حق المؤلّف وحقوق التأليف والنشر والطباعة، كلّها مكفولة للوكالة الوطنية للأمن السيبراني في دولة قطر.

وعليه، فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نشر أي جزء من هذا الكُتَيّب، أو الاقتباس منه، أو نَسْخ أي جزء منه، أو نقله كلياً أو جزئياً في أي شكل وبأيّ وسيلة، سواء بطُرق إلكترونية أو آلية، بما في ذلك التصوير الفوتوغرافي، أو التسجيل، أو استخدام أي نظام من نُظُم تخزين المعلومات واسترجاعها، سواء من الأنظمة الحالية أو المُبتكَرة في المستقبل، إلا بعد الرجوع إلى الوكالة، والحصول على إذنٍ خَطّي منها.

ومَنْ يُخالِف ذلك يُعرِّض نفسه للمُساءَلة القانونية.

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

00974 404 663 62
00974 404 663 79
academy@ncsa.gov.qa
www.ncsa.gov.qa/

يناير 2025م
الدوحة، قطر

◆ عزيزي المشارك

في ظلّ التطوُّر التكنولوجي المتسارع، ودخول الإنترنت إلى مختلف مجالات الحياة؛ أصبحت التهديدات السيبرانية تُواجِه مختلف شرائح المجتمع، ما يتطلَّب العمل على تعزيز الوعي بمفاهيم السلامة الرقمية؛ التي تُعدّ الدّرع الذي يحمي المجتمع من هذه التهديدات.

وفي سياق جهود «المبادرة الوطنية للسلامة الرقمية» لتعزيز مؤشرات السلامة الرقمية في المجتمع؛ تُقدِّم الوكالة الوطنية للأمن السيبراني هذا الكُتَيِّب، والذي يتضمَّن مجموعةً من النصائح والإرشادات العامَّة المتعلّقة بالسلامة الرقمية.

الفهرس	رقم الصفحـة

مُقدّمـــة

تُعدّ حماية البيانات أمراً ضرورياً في عصرنا الحالي؛ خاصةً مع التطور التكنولوجي المتسارع، والكَمّ المتزايد من البيانات المجمَّعة التي تخضع للكثير من المُعالَجات، وهو ما استدعى وجود لوائح تنظيمية لحماية خصوصية وأمن البيانات، سواء للأفراد أو المنظمات. وتعمل هذه اللوائح على تحديد إرشادات صارمة لمعالجة البيانات والتعامل معها، وقد تطورت على مدار السنوات الماضية مواكبةً للتغيرات الطارئة بالمجال الرقمي.

وتكتسب حماية البيانات أهميتها من خلال عدة محاور؛ يأتي في مقدمتها مسألة الامتثال للوائح المنظِّمة للبيانات في بلدان العالم، والتي تُلزم المنظمات بعدة اشتراطات، وإلا عُوقبت بغرامات باهظة وإجراءات قانونية صارمة، بخلاف تضرُّر سمعة المنظمة.

هذا إلى جانب أهمية حماية البيانات من الهجمات السيبرانية التي اتَّخذت أشكالاً أكثر تنوعاً وخطورةً، وتنتج عنها خسائر مالية كبيرة للمنظمات في حال افتقرت لإجراءات أمنية تستطيع مواجهة هذه الهجمات وحماية البيانات بها.

ومن الأمور المرتبطة بحماية البيانات: مسألة حماية بيانات العملاء؛ حيث تحتفظ المنظمات بالكثير من بيانات العملاء، مثل: الأسماء والعناوين ومعلومات الدفع، ومن هنا تكتسب هذه البيانات أهمّيتها لضمان عدم تسرُّبها أو خرقها، ومِن ثَم إساءة استخدامها، وما ينتج عن ذلك من خسائر مالية وتضرُّر سُمعة المنظمة والعملاء معاً.

ما سبق يؤكد أن حماية البيانات داخل المنظمات من التسرُّب والخَرْق مُهمة لضمان استمرارية الأعمال بها، فأيّ تعطُّل لمسار العمل يؤدّي إلى توقُّف وتعطُّل كامل، وبالتالي تراجع الإنتاجية وتعطل الأعمال التشغيلية والإدارية.

ونشير هنا إلى أن تسرُّب البيانات يحدث عندما تُكشَف البيانات الحسّاسة عن غير قصد للجمهور في أثناء النقل، أو في أثناء الاستخدام، وقد يتم ذلك خلال عملية نقل البيانات عبر رسائل البريد الإلكتروني، أو مكالمات واجهة برمجة التطبيقات، أو غُرَف الدردشة، وغيرها من وسائل الاتصال الأخرى. أو قد يتم كشف البيانات خلال فترات عدم النشاط، ويحدث ذلك نتيجة للتخزين السحابي الذي تم تكوينه بشكل غير صحيح أو قواعد البيانات غير الآمِنَة، أو بسبب الأجهزة المفقودة. كما أن البيانات المكشوفة قَيْد الاستخدام هي أيضاً عُرْضة للتسرُّب مثل: البيانات الموجودة على الطابعات ولقطات الشاشة ومُحرّكات أقراص USB.

01

الفصل الأول

تسرُّب البيانات
Data Leakage

- أولاً: مفهوم تسرُّب البيانات Data leakage concept.
- ثانياً: الفرق بين تسرُّب البيانات Data Leakage وخرق البيانات Data Breach.

تسرُّب البيانات Data Leakage

يُعدّ تسرُّب البيانات من أخطر التهديدات التي تُواجه الأفراد والمؤسسات في العصر الرقمي. يحدث هذا النوع من الحوادث عندما يتمّ الكشف عن معلومات حسّاسة أو سرّية لجهات غير مصرَّح لها، سواء كان ذلك بسبب هجمات سيبرانية أو أخطاء بشرية، أو ثغرات في الأنظمة الأمنية.

تسرُّب البيانات يمكن أن يؤدّي إلى خسائر مالية ضخمة، وتشويه السمعة، واستغلال المعلومات الشخصية أو التجارية بشكل غير قانوني. وفي ظل التزايد المستمرّ للأنشطة الرقمية؛ أصبحت حماية البيانات أولوية قصوى للحفاظ على الأمان الرقمي والخصوصية في مختلف القطاعات، بما في ذلك الشركات والمؤسسات الحكومية.

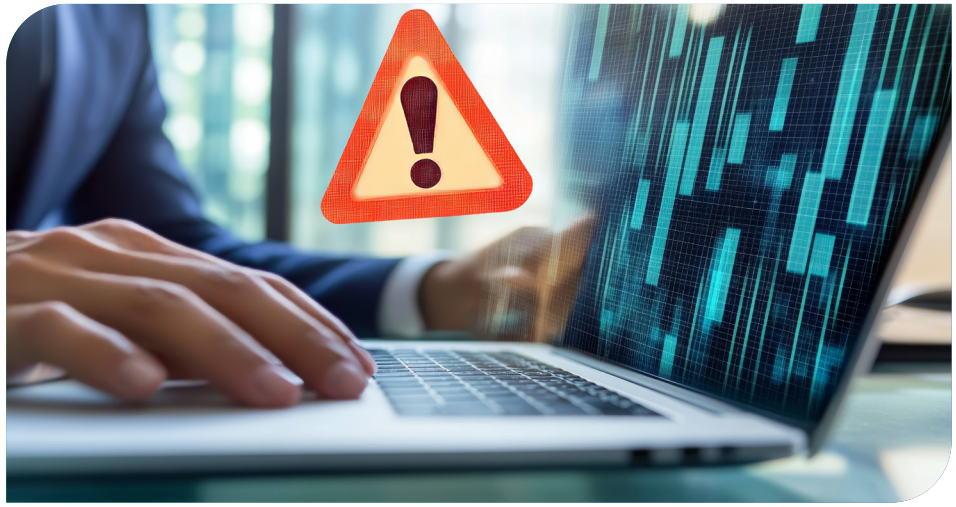
أولاً: مفهوم تسرُّب البيانات Data Leakage Concept

يحدث تسرُّب البيانات عند كشف البيانات المهمة لأشخاص غير مصرَّح لهم نتيجة حدوث أخطاء داخل المنظمة، وعادةً ما يحدث هذا بسبب ضعف أمان البيانات أو الأنظمة غير المحدَّثة، أو عدم تدريب الموظفين بشكلٍ كافٍ؛ حيث يؤدي تسرُّب البيانات إلى سرقة الهويات سواء للموظفين أو العملاء، أو خرق البيانات، أو تثبيت برمجيات ضارَّة مثل برمجية الفدية.

وعلى الرغم من طبيعته العرضية وافتقاره إلى سوء النية؛ إلا أنه يمكن أن يتسبَّب تسرُّب البيانات في إلحاق ضرر بالغ بالمنظمات وأعمالها؛ إذ يؤدي إرسال ملفّ مهمّ بالخطأ لجهات غير مصرَّح لها إلى تداوله ووقوعه في أيدي المجرمين الإلكترونيين، واستغلاله فيما بعد في تنفيذ هجمات مثل هجوم الفدية.

احذر!

يؤدّي تسرُّب البيانات إلى سرقة الهويات سواء للموظفين أو العملاء أو تثبيت برمجيات ضارَّة مثل برمجية الفدية.



ومن أمثلته:

1. عندما يقوم موظّف داخل المنظمة بإرسال مستند مُهمّ عن طريق الخطأ إلى أطراف خارجية عبر البريد الإلكتروني.
2. عندما يتم نشر بيانات مهمَّة نتيجة إعدادات خاطئة في تطبيق أو نتيجة خطأ بشريّ، ما يجعلها متاحة أمام الجميع.
3. ظهور بيانات مهمَّة في خلفيات صُوَر تم التقاطها عن طريق الخطأ بكاميرات شخصية نشرت للعامة.

ثانياً: الفرق بين تسرُّب البيانات Data Leakage وخرق البيانات Data Breach

غالباً يتم استخدام نفس المصطلحين بالتبادل للتعبير عن نفس الفكرة؛ إلا أن هناك فروقاً بينهما. ففي حين يُشير تسرُّب البيانات وخرق البيانات إلى وصول أشخاص غير مُصرَّح لهم إلى البيانات المهمة؛ فإن السبب يُحدّد نوعية الانتهاك ما إذا كان تسرباً أم خرقاً.

إذ يحدث تسرُّب البيانات عندما يكشف مصدر داخل المنظمة عن بيانات. أما خرق البيانات فيحدث عندما يخترق مصدر خارجي النظام بواسطة هجوم سيبراني، ما يعني أنه يُنظَر لتسرُّب البيانات كحادث عرضيّ نتيجة خطأ داخلي أو إهمال، بينما يُعدّ خرق البيانات هجوماً مقصوداً. وفي بعض الأحيان يَصْعُب التمييز بين التسرُّب والخرق؛ لأن مجرمي الإنترنت يستخدمون البيانات المسرَّبة في تنفيذ عملية خرق واسعة النطاق للبيانات. فعلى سبيل المثال، عند اختراق حساب بريد إلكتروني واحد فيمكنهم حينها تنفيذ عمليات احتيال عبر البريد الإلكتروني التجاري مثل هجمات برمجيات الفدية.

احذر!

في حال إرسال ملفّ مُهمّ بالخطأ لجهات غير مُصرَّح لها يُؤدّي ذلك إلى تداوله ووقوعه في أيدي مجرمي الإنترنت واستغلاله فيما بعد في تنفيذ هجمات مثل هجوم الفدية والاحتيال.

إذاً يحتاج مجرمو الإنترنت إلى تسرُّب بيانات واحد فقط لتحويله إلى خرق هائل للبيانات، بما يشكل تهديداً خطيراً للمنظمات[1]. وتُصنّف خروقات البيانات وفق نوع ناقل الهجوم المستخدَم ومن ارتكب الهجوم، **فهناك نوعان رئيسيان من خروقات البيانات:**

1. خروقات البيانات التي تصدر من جهة تهديد خارجية.
2. خروقات البيانات التي تَصْدر عن تهديدات داخلية مرتبطة بالمنظمة، وتنقسم إلى: الهجمات الخبيثة، وتتم بواسطة موظَّف غاضب من المنظمة، وهجمات الإهمال نتيجة كلمات المرور الضعيفة، وحالات التوظيف، وتتضمن قيام مجرمي الإنترنت بإغراء الموظفين داخل المنظمة؛ لمساعدتهم على مهاجمة الشبكة وسرقة البيانات.

وبناء على ما سبق، يتبيّن أن خروقات البيانات ليست عرضية، بل هجمات ضارَّة تَستهدف الإضرار بالمنظمات.

احذر!

يحتاج مجرمو الإنترنت إلى تسرب بيانات واحد فقط لتحويله إلى خرق هائل للبيانات، بما يُشكّل تهديداً خطيراً للمنظمات.

1. Data Breach Versus Data Leak: What's The Difference?, 2024. Follow link: https://www.teramind.co/blog/data-breach-vs-data-leak/

ومن طرق خرق البيانات:

1. هجمات برمجيات الفدية الأكثر شيوعاً للحصول على المال مقابل البيانات المسروقة، خاصة في حال لم تمتلك المنظمات نسخةً احتياطيةً من البيانات.
2. هجمات الهندسة الاجتماعية التي تستهدف العاملين في المنظمات؛ لخداعهم، والتسلل إلى البيانات الحساسة عبر اختراق الشبكة، وإذا لم ينجحوا في هذا يلجأ المهاجم إلى هجمات حشو بيانات الاعتماد؛ حيث تحاول هجمات القوة الغاشمة تخمين كلمات مرور العاملين والدخول إلى الشبكة، إضافةً إلى استخدام برمجيات ضارَّة مثل أحصنة طروادة لاختراق النظام أو اختراق الخوادم من خلال تنفيذ هجمات سيبرانية معقَّدة.

احذر!

يُؤدّي استخدام الموظفين نفس كلمة المرور لحسابات متعددة إلى الوقوع ضحية هجمات حشو بيانات الاعتماد، مما يسهّل عملية اختراق المنظمات وسرقة بياناتها.

02

الفصل الثاني

تسـرُّب البيـانـــات فـي المنظـمـــات

- أولاً: **أسباب تسرُّب البيانات في المنظمات.**
- ثانياً: **أنواع البيانات المسرَّبة في المنظمات.**

تسرُّب البيانات في المنظمات

يُعدّ تسرُّب البيانات في المنظمات تهديداً متزايداً يُؤثّر بشكلٍ كبيرٍ على أمن المعلومات وسلامة العمليات. يحدث تسرُّب البيانات عندما تُكشَف أو تُسرَّب معلومات حساسة، مثل بيانات العملاء أو الخطط الإستراتيجية أو التفاصيل المالية، إلى جهات غير مصرَّح لها. قد ينتج ذلك عن هجمات سيبرانية، أخطاء بشرية، أو ثغرات في البنية التحتية الأمنية. وتتعرَّض المنظمات التي تواجه هذه الحوادث لخسائر مالية فادحة، وتضرُّر سُمعتها، وفقدان ثقة العملاء. لذا، أصبحت حماية البيانات إحدى أهم أولويات الشركات لضمان استمرارية العمل وتقليل المخاطر في بيئة رقمية مليئة بالتحديات.

أولاً: أسباب تسرُّب البيانات في المنظمات

1. ضعف البنية التحتية

عدم اعتماد البنية التحتية في المؤسسات على معايير حديثة فيما يتعلق بأمن المعلومات قد يؤدي إلى وجود إعدادات أو أذونات خاطئة ما ينتج عنه تسرُّب للبيانات[1].

2. هجمات الهندسة الاجتماعية Social Engineering Attacks

على الرغم من أن خرق البيانات ينتج عن هجمات سيبرانية، لكن قد يلجأ المجرمون إلى طرق مماثلة لتسريب بيانات المنظمات لشَنّ هجمات أخرى، مثل رسائل البريد الإلكتروني التصيدية التي تؤدي للوصول إلى بيانات تسجيل الدخول الخاصة ببعض الموظفين، وبالتالي خرق بيانات المنظمة.

احذر!

يلجأ مجرمو الإنترنت إلى طرق عديدة لتسريب بيانات المنظمات لشنّ هجمات أخرى، مثل رسائل البريد الإلكتروني التصيدية التي تؤدّي للوصول إلى بيانات تسجيل الدخول الخاصة ببعض الموظفين، وبالتالي خرق بيانات المنظمة.

1. What Is a Data Leak? How They Happen and How To Prevent Them. Follow link: https://abnormalsecurity.com/glossary/data-leak

وغالباً ما تستخدم الجهات المنفِّذة للهجوم الإلكتروني تقنيات الهندسة الاجتماعية لخداع الموظفين لتقديم معلومات حساسة؛ من خلال تظاهر مجرم الإنترنت بأنه زميل في العمل أو متخصّص في قسم تكنولوجيا المعلومات.

وتعمد هجمات الهندسة الاجتماعية إلى سرقة بيانات تسجيل الدخول أو أرقام الهواتف أو أسماء الموظفين الذين يتمتعون بامتيازات الوصول إلى البيانات[1].

حقائق وأرقام

تم بيع 500,000 نسخة من بيانات اعتماد زووم Zoom على الويب المظلم، ووصل سعر كلمات المرور إلى قِيَم زهيدة بسبب وَفْرة العرض من خلال هجمات حَشو بيانات الاعتماد؛ حيث يقوم مجرمو الإنترنت بتسجيل الدخول إلى زووم Zoom بواسطة حسابات تم تسريبها في خروقات البيانات القديمة، ليتم بعد ذلك تجميع عمليات تسجيل الدخول الناجحة في قوائم يتم بيعها للمتسللين الآخرين[2].

3. كلمات المرور الضعيفة

يميل بعض المستخدمين إلى استخدام نفس كلمة المرور لحسابات متعددة؛ لسهولة تذكُّرها، وبالتالي عند وقوع هجوم حشو بيانات الاعتماد يؤدي ذلك إلى كشف عدة حسابات واختراق المنظمات وسرقة بياناتها.

1. Data Leakage: Common Causes, Examples & Tips for Prevention. Follow link: https://www.bluevoyant.com/knowledge-center/data-leakage-common-causes-examples-tips-for-prevention
2. Over 500,000 Zoom accounts sold on hacker forums, the dark web. Follow link: https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/

4. الأجهزة المفقودة

في حال فقد أحد الموظفين جهازاً يتضمَّن معلومات حساسة خاصَّة بالمنظمة يُعدّ ذلك بمثابة اختراق محتمَل للبيانات؛ لأنه يُسهّل مهمة المهاجم في الوصول إلى بيانات المنظمة وخَرْقها.

5. الثغرات الأمنية في البرامج والتطبيقات

تُسبِّب الثغرات الأمنية نقاط ضَعْف خطيرة في المؤسسات، ومنها الثغرات غير المكتشفة، فقد يستغل مجرمو الإنترنت هذه الثغرات في تنفيذ هجمات مُتعدّدة تستهدف بيانات المؤسسات.

6. الأجهزة القديمة

هذه الأجهزة تكون بنظم تشغيل قديمة، ما يسهل خرقها، كما أن معايير الأمان فيها تكون منخفضة، ما يُشكّل نقطة ضعف يمكن أن تتسرب البيانات عبرها.

احذر!

استخدام الموظفين الأدوات والأجهزة الشخصية مثل الطابعات المنزلية لطباعة بيانات حسّاسة تخصّ المنظمة يُعرّضها لخطر تسرُّب البيانات وهجمات الفدية، وغيرها.

احذر!

في حال فقد جهاز يتضمَّن معلومات حساسة خاصة بالمنظمة يُعدّ ذلك بمثابة خرق محتمَل للبيانات؛ لأنه يُسهّل مهمة المهاجم في الوصول إلى بيانات المنظمة وخرقها.

ثانياً: أنواع البيانات المسرَّبة في المنظمات

1. معلومات التعريف الشخصية Personally identifiable information (PII)

وهي المعلومات أو السجلات التي تُحدّد هوية الموظفين والعملاء مثل الأسماء وأرقام الهواتف والعناوين وعنوان البريد الإلكتروني، والهدف هو سرقة الهوية، وتنفيذ عمليات الاحتيال، فغالباً ما تظهر معلومات تحديد الهوية الشخصية في حالات تسرُّب البيانات.

2. البيانات المالية Financial data

جميع البيانات الخاصة بالشؤون المالية أو المصرفية للمنظمات؛ مثل المعلومات الضريبية والفواتير.

3. بيانات اعتماد الحساب أو تسجيل الدخول Account credentials

تشمل معلومات تسجيل الدخول إلى حساب المستخدمين بما في ذلك أسماؤهم وكلمات المرور ورسائل البريد الإلكتروني، وهي الأكثر طلباً لقدرتها على مساعدة مجرمي الإنترنت في تنفيذ عمليات الاستيلاء على الحسابات وخرق البيانات.

4. معلومات المنظمة Organization information

تشمل المعلومات الداخلية التي يتم إنشاؤها وتخزينها بواسطة المنظمة، والتي تتضمّن معلومات الأعمال المهمة مثل الاتصالات الداخلية، والسجلات السرية، ومقاييس الأداء، وملاحظات الاجتماعات، وسجلات الموارد البشرية، وكل ما يتعلق بأعمال المنظمة.

5. الأسرار التجارية والملكية الفكرية Trade secrets and intellectual property (IP)

هي معلومات سرية للغاية ومحمية يؤدّي الكشف عنها إلى تعريض المنظمات للخطر، مثل الأبحاث السرية، وبراءات الاختراع، والخطط، ومواد الاختبار، وتصميمات المشاريع المستقبلية، وكود المصدر للبرمجيات والتكنولوجيا الاحتكارية، وجميع المعلومات الإستراتيجية الخاصة بالمنظمة[1].

1. Check Fraud - Types, Reporting, and Prevention Strategies, March 2024. on site: https://www.tookitaki.com/glossary/check-fraud

هل تعلم؟

في عام 2021م، كشفت الأبحاث أن 74% من الشركات الكبيرة و61% من الشركات الصغيرة تعرَّضت لخرق البيانات، كما سجَّلت نِسَب خرق البيانات في العالم زيادةً بنسبة تزيد على 70% في الربع الثالث من عام 2022م.

03

الفصل الثالث

إستراتيجيات حماية البيانات السرية من التسرب

- أولاً: **اكتشاف تسرُّب البيانات في المنظمة.**
- ثانياً: **إجراءات عامة لحماية البيانات من التسرب.**

إستراتيجيات حماية البيانات السرية من التسرب

حماية البيانات السرية من التسرُّب تُعدّ جزءاً حيوياً من إستراتيجيات الأمن السيبراني الحديثة. مع تزايد الاعتماد على التكنولوجيا في إدارة المعلومات الحسّاسة؛ مثل: البيانات المالية، الخطط الإستراتيجية، وبيانات العملاء. ولذا أصبح من الضروري اتخاذ تدابير صارمة لضمان عدم وقوعها في أيدٍ غير مُصرَّح لها.

تسرُّب هذه البيانات يمكن أن يُؤدّي إلى خسائر مالية جسيمة وتشويه سُمْعة المنظمة. لذلك، تتضمَّن حماية البيانات السرية استخدام تقنيات التشفير، وتعزيز سياسات الوصول، وتدريب الموظفين على الممارسات الآمنة، وتحديث الأنظمة الأمنية باستمرار. هذه الجهود تُسْهم في الحفاظ على سرية المعلومات، وحماية المنظمة من التهديدات الخارجية.

احذر!

عند رصد زيادة في محاولات تسجيل الدخول الفاشلة، أو محاولات الوصول غير المصرَّح به إلى البيانات؛ يجب على الموظف سرعة إبلاغ الجهة المسؤولة عن الأمن السيبراني داخل المنظمة.

أولاً: اكتشاف تسرُّب البيانات في المنظمة

هناك مؤشرات تكشف عمليات تسرُّب البيانات بشكل استباقي، وهي تُمثِّل أيّ نشاط خارج عن المألوف يُوحي بوجود مشكلة مثل[1]:

- حركة مرور أعلى من المعتاد على الموقع.
- مطالبات استرداد كلمة المرور غير المتوقَّعة.
- زيادة في محاولات تسجيل الدخول الفاشلة.
- تراجع عدد رسائل البريد الإلكتروني.
- محاولات الوصول غير المصرَّح به إلى البيانات.
- محاولات الدخول إلى أنظمة الشركة خارج ساعات العمل المتعارَف عليها.
- مشكلات في أداء النظام؛ فالعديد من التهديدات السيبرانية مثل هجمات DDoS تُؤثّر على أداء الشبكة وسرعتها، وبالتالي فإن بطء الأداء دون مُبرِّر يعني أن النظام يتعرَّض للهجوم.
- زيادة إجمالية في محاولات تسجيل الدخول.

احذر!

يُعدّ فقدان الملفات بشكل مفاجئ، وعدم القدرة على الوصول إلى معلومات مُحدَّدة أحد مؤشرات عمليات تسرُّب البيانات داخل المنظمات.

1. How to Detect a Data Breach (5 Critical Steps). Follow link: https://www.breachsense.com/blog/data-breach-detection/

- وجود الملفات المشفَّرة نتيجة هجوم الفدية.
- وجود تغييرات مفاجئة في قاعدة البيانات.
- فقدان الملفات بشكلٍ مفاجئ.
- عدم القدرة على الوصول إلى معلومات محدَّدة.
- زيادة عدد رسائل البريد الإلكتروني التصيدية الموجَّهة إلى موظفي المنظمة.

هل تعلم؟

في عام 2020م، وقع موظفو منصة تويتر (إكس حالياً) ضحية هجوم تصيُّد احتيالي تسبَّب في السماح لمجرمي الإنترنت بالوصول إلى 130 حساباً خاصّاً ومؤسسياً على المنصة، مثل حساب إيلون ماسك، وبيل جيتس[1].

وبدأ الهجوم برسالة على البريد الإلكتروني ادَّعت أنها من فريق تكنولوجيا المعلومات الخاص بتويتر، ولعدم تحقُّق الموظف الداخلي من الرسالة نجَح الهجوم السيبراني.

1. Hackers targeted Twitter employees to hijack accounts of Elon Musk, Joe Biden and others in digital currency scam. Follow link: https://www.cnbc.com/2020/07/15/hackers-appear-to-target-twitter-accounts-of-elon-musk-bill-gates-others-in-digital-currency-scam.html

ثانياً: إجراءات عامّة لحماية البيانات من التسرُّب

تحتاج المنظمات إلى مجموعة من الإجراءات المنظِّمة لحماية بياناتها المتنوعة، والتي تُعدّ أحد أصولها المهمَّة حفاظاً عليها من الفقد أو التسرب والوقوع في أيدي مجرمي الإنترنت الذين يستغلون مثل هذه البيانات في تنفيذ المزيد من الهجمات السيبرانية للحصول على المال، مثل هجوم الفدية.

ومن أبرز إجراءات الحماية ما يلي:

1. تشفير البيانات

يُقصَد بالتشفير إجراء تحويل للبيانات المهمَّة إلى رموز؛ لمنع الوصول غير المصرَّح به، وتشمل العملية جميع البيانات الحساسة مثل بيانات العملاء والبيانات المالية والملكية الفكرية؛ حيث يقوم تشفير البيانات بتحويل البيانات القابلة للقراءة إلى تنسيق غير قابل للقراءة؛ باستخدام خوارزميات مُعيّنة. ولفكّ تشفير هذه البيانات وقراءتها يتطلَّب الأمر الحصول على المفتاح الذي يفكّ الخوارزمية المستخدَمة[1].

1. Who should encrypt the data in my company?. Follow link: https://www.sealpath.com/blog/data-encryption-for-enterprises/

2. النسخ الاحتياطي للبيانات

تساعد عملية النسخ الاحتياطي المنتظمة للبيانات في تعزيز قدرة المنظمات على التعافي من حالات خرق وتسرُّب البيانات بشكل أسرع وبتكلفة أقل. لهذا يُنصَح دائماً بعمل نُسَخ احتياطية من البيانات بانتظامٍ، مع الحرص على تخزينها في أماكن آمِنَة[1].

3. توعية موظفي المنظمة

من ممارسات الحماية السيبرانية الأساسية: توعية وتثقيف الموظفين داخل المنظمة من أجل أفضل ممارسات حماية للبيانات، مثل: إنشاء كلمات مرور قوية، والتمييز بين رسائل البريد الإلكتروني الآمِنَة والتصيدية.

4. ضوابط الوصول إلى البيانات

من الأمور التي ينبغي أن تُؤخَذ في الاعتبار: مسألة تقييد الوصول إلى البيانات الحساسة في المنظمة، لهذا على المنظمات التأكُّد من وصول الموظفين بها إلى البيانات الضرورية لمهام عملهم فقط، وألّا تمنحهم تصريحاً موسعاً للوصول إلى جميع البيانات.

1. Paul Kirvan, How can your ransomware backup strategy improve?, Feb 2020. Follow link: https://www.techtarget.com/searchdatabackup/answer/How-can-your-ransomware-backup-strategy-improve?utm_source=google&int=off&pre=off&utm_medium=cpc&utm_term=GAW&utm_content=sy_lp01252024GOOGOTHR_GsidsDataBackup_ExaGrid_Essential_IIO244839_LI2764124&utm_campaign=ExaGrid_EG_sDB_WW&Offer=sy_lp01252024GOOGOTHR_GsidsDataBackup_ExaGrid_Essential_IO244839_LI2764124&gad_source=1&gclid=EAIaIQobChMI5sep5O_lhgMVKwMGAB0gTQXxEAAYAiAAEgLR2PD_BwE

5. التدقيق الأمني المنتظم

تسهم عمليات التدقيق الأمني المنتظمة في تحديد نقاط الضعف المتعلقة بحماية البيانات، ومن ثم الإجراءات التي يجب اتباعها لمعالجة هذه النقاط في المنظمات[1].

فعملية التحقُّق المنتظمة، واعتماد نهج أمان الثقة المعدومة، يُسهمان في منع الوصول غير المصرَّح به إلى البيانات الحساسة في المنظمات.

6. المصادقة متعددة العوامل

إن سياسة كلمة المرور القوية أمر جيد، ولكن لا تعتمد عليها وحدها؛ حيث يضمن تنفيذ التحقق متعدد العوامل أن تسرُّب كلمة المرور لا يكفي للتسبُّب في خرق البيانات[2].

وتنبع أهمية استخدام المصادقة متعددة العوامل من تنوُّع طرق حصول مجرمي الإنترنت على بيانات تسجيل الدخول، فهي طريقة مصادقة تطلب من الموظفين داخل المنظمات أو الأطراف الخارجية تقديم عاملَي تحقُّق أو أكثر لتأكيد هويتهم قبل الوصول إلى البيانات الحساسة أو الحسابات والتطبيقات التابعة للمنظمة، وبدلاً من طلب اسم مستخدِم وكلمة مرور فقط للتحقُّق من هوية الموظف يتم التحقّق من معلومات إضافية مثل رمز المرور لمرة واحدة أو رمز التشفير أو بصمة الإصبع.

1. Kevin Mitch Group, Importance of Data Protection within the Organization, March 2023. Follow link: https://www.linkedin.com/pulse/importance-data-protection-within-organization-kevin-mitch-group/
2. How Security Leaders Can Use Multi-Factor Authentication to Protect Sensitive Data. Follow link: https://www.terranovasecurity.com/blog/multi-factor-authentication-protect-sensitive-data

وهناك ثلاثة أنواع رئيسة من عوامل المصادقة:

- المعلومات التي يعرفها الموظف أو الطرف الخارجي المتعاقد مع المنظمة، مثل كلمات المرور أو الرقم السري.
- أشياء يعلمها الموظف أو الطرف الخارجي المتعاقد مع المنظمة: رمز التشفير.
- شيء خاص مثل بصمة الإصبع، أو الصوت، أو بصمة الوجه.

7. المصادقة متعددة العوامل Adaptive Multi-Factor Authentication

يُطلَق عليها أيضاً المصادقة القائمة على المخاطر، وهي تقنية أمان متقدّمة تتطلب من الموظف داخل المنظمة أو أيّ من المتعاقدين معها بالخارج تقديم عاملَي تحقُّق أو أكثر من أجل الوصول إلى حساباته، وتسمى بـ "التكيفية"؛ لأنها تقوم بضبط عوامل المصادقة وفق المخاطر المختلفة مثل نوع الجهاز ووقت الوصول وأمن الشبكة، وأنماط سلوك الموظفين، والموقع الجغرافي، ونظام التشغيل... إلى غير ذلك، وذلك بخلاف المصادقة متعدّدة العوامل المعتادة[1].

على سبيل المثال: يعمل بعض موظفي المنظمة عن بُعْد، أو من المنزل بواسطة جهاز حاسوب محمول وشبكة اتصال Wi-Fi عامة، وباستخدام المصادقة متعددة العوامل يمكن للمنظمة تحديد مجموعة واحدة من الإجراءات المتعلقة بالمصادقة في حال عمل الموظف من المنزل، وأخرى مغايرة في حال قيامه بالعمل في أثناء السفر.

1. What is Adaptive Multi-Factor Authentication (MFA)?. FOLLOW LINK: https://www.cyberark.com/what-is/adaptive-mfa/

8. مراقبة مخاطر الطرف الثالث

من الأمور التي يجب على المنظمات مراعاتها: مراقبة مخاطر الطرف الثالث؛ فقد تحدث هجمات سلسلة التوريد عندما يتعرَّض أحد بائعي الطرف الثالث لخرق بيانات؛ مما يؤدي إلى تسرُّب البيانات على نطاق واسع.

حقائق وأرقام

في عام 2020م، بلغ متوسط تكلفة خرق البيانات 3,9 مليون دولار أمريكي.

فالمنظمات حالياً -خاصةً مع الدخول في الحوسبة السحابية، والعمل عن بُعْد، والنُّظم البيئية لسلسلة التوريد العالمية-؛ زاد اعتمادها على خدمات الطرف الثالث من أجل تحقيق الكفاءة وزيادة الإنتاجية، وتقديم السلع أو الخدمات، لكن هذا الاعتماد المتزايد يُرافقه ارتفاع مماثل في فرص التهديدات السيبرانية المتعلقة بالطرف الثالث الذي يتعامل مع بيانات المنظمة الحساسة.

9. تحديد وتصنيف البيانات الحساسة

على المنظمة تحديد أنواع البيانات التي تتعامل معها مثل المعلومات الشخصية والسجلات المالية والملكية الفكرية والأسرار التجارية، وتصنيف البيانات وفق أهميتها ومدى حساسيتها والتأثير المحتمل في حالة تسرُّبها، مع وضع إرشادات واضحة للتعامل مع كلّ تصنيف من تصنيفات البيانات، والتأكد من فَهْم الموظفين لهذا.

10. تثبيت برامج مكافحة الفيروسات والبرمجيات الضّارَّة

من إجراءات الحماية المطلوبة للبيانات، قيام المنظّمة بتثبيت برامج مكافحة الفيروسات والبرمجيات الضّارَّة مع التأكُّد من كونها فعّالة على جميع نقاط النهاية، بما في ذلك الخوادم وأجهزة الحاسوب المكتبية والمحمولة، وكذلك الالتزام بتحديث هذه البرامج بانتظام للتأكُّد من قدرتها على اكتشاف نقاط الضعف والتهديدات، ومعالجتها بأسرع وقت.

11. الاستجابة للحوادث واكتشاف تسرُّب البيانات

يتم ذلك من خلال وضع خطة للاستجابة السريعة للحوادث بهدف خفض تأثيرها على المنظمة، وهذا يتطلب بناء فريق فعّال للاستجابة للحوادث، شريطة أن يكون مُتعدّد الوظائف، ويضم أعضاء من أقسام تكنولوجيا المعلومات والشؤون القانونية والعلاقات العامة، والإدارات الأخرى ذات الصلة، لوضع خطة واضحة تُحدّد الأدوار والمسؤوليات والإجراءات التي يجب اتباعها عند تسرُّب البيانات[1].

1. Preventing and Detecting Data Leaks: The Complete Guide. Follow link: https://flare.io/learn/resources/blog/data-leakage-prevention/

التمارين تعتمد على المادة العلمية المقدَّمة في سياق هذا الكتيب، وهي مذكورة هنا بدون حل، وتم إرفاق الحل في نهاية الكُتَيِّب.

التمرين الأول

• اختر الإجابة الصحيحة

1. يُقصَد بـ"تكنولوجيا المعلومات الظلية Shadow IT" ...

1. استخدام أنظمة تكنولوجيا المعلومات والأجهزة والبرامج والتطبيقات والخدمات دون تصريح مباشر من قسم تكنولوجيا المعلومات في المنظمات.
2. لجوء المهاجم إلى هجمات حشو بيانات الاعتماد لتخمين كلمات مرور العاملين والدخول إلى الشبكة.
3. قيام موظف ما بالتدخل المباشر بعيداً عن المختصين المعتمدين للتعامل مع المشكلة وإصلاحها، أو اللعب في إعدادات الأمان.
4. (1)، (3) معاً.

2. من أسباب تسرُّب البيانات في المنظمات .....

1. وجود إعدادات أو أذونات خاطئة.
2. الاحتفاظ بإصدار قديم من برنامج ما.
3. رسائل البريد الإلكتروني التصيدية.
4. جميع ما سبق.

3. تتضمَّن الملكية الفكرية ما يلي .....

1. الأبحاث السرية.
2. موادّ الاختبار.
3. كود المصدر للبرمجيات.
4. المعلومات الإستراتيجية الخاصة بالمنظمات.
5. جميع ما سبق.

4. تتمحور فوائد أدوات منع تسرُّب البيانات حول .....

1. التصنيف اليدوي للبيانات، مما يساعد على منع مشاركة البيانات الحساسة مع غير المصرَّح لهم.
2. فحص شبكة الويب المظلمة والعادية للعثور على تسريبات البيانات قبل استخدامها في أيّ هجوم سيبراني.
3. تمكين المنظمات من التحايل على معايير وقوانين ولوائح حماية البيانات، مع إمكانية إعداد التقارير المزيَّفة التي تحتاجها المنظمة لإكمال عمليات تدقيق الامتثال.
4. جميع ما سبق.

التمرين الثاني

اكتب كلمة (صحيح) أمام العبارة الصحيحة، وكلمة (خطأ) أمام العبارة الخاطئة، وصحّح العبارة الخاطئة

1. يتم تسرُّب البيانات عند كشف البيانات المهمة لأشخاص مصرَّح لهم نتيجة حدوث أخطاء داخل المنظمة. (.....)

2. يحدث خرق البيانات عندما يخترق مصدر خارجي النظام بواسطة هجوم إلكتروني. (.....)

3. يحتاج مجرمو الإنترنت إلى عدة تسريبات للبيانات للتمكُّن من القيام بعملية اختراق هائل للبيانات، بما يشكل تهديداً خطيراً للمنظمات. (.....)

4. تُعدّ هجمات برمجيات الفدية هي الأكثر شيوعاً للحصول على المال مقابل البيانات المسروقة، خاصة في حال لم تمتلك المنظمات نسخة احتياطية من البيانات. (.....)

5. لا تؤدي الأجهزة الإلكترونية المفقودة مِن قِبَل أحد الموظفين إلى تهديد المنظمة التي يعمل بها لصعوبة وصول المهاجم إلى بياناتها وخرقها. (.....)

6. يصعب على مجرمي الإنترنت خرق بيانات المنظمة في حال فقد الأجهزة الإلكترونية. (.....)

7. لجوء الموظفين لاستخدام الأدوات والأجهزة الشخصية مثل الطابعات المنزلية في العمل يحمي المنظمة من تسرُّب البيانات. (.....)

8. محاولات استعادة كلمة المرور التي لم يبدأها الموظف تُعدّ أحد مؤشرات تسرُّب البيانات. (.....)

9. يمكن القيام بتشفير البيانات خلال عملية نقلها سواء بين الشبكات أو من مكان العمل إلى السحابة، أو من جهاز إلى جهاز داخل المنظمة. (.....)

التمرين الثالث

أكمل العبارات التالية

1. يؤدي تسرُّب البيانات إلى ..... أو ..... أو ..... .
2. من أنواع البيانات المسربة في المنظمات ..... ، ..... ، ..... .
3. قد تصدر خروقات البيانات عن تهديدات داخلية مرتبطة بالمنظمة، وتنقسم إلى: ..... وتتم بواسطة موظف غاضب من المنظمة، و..... نتيجة كلمات المرور الضعيفة، و..... والتي تضمن قيام مجرمي الإنترنت بإغراء الموظفين داخل المنظمة لمساعدتهم على مهاجمة الشبكة وسرقة البيانات.
4. يمكن حماية بيانات المنظمات من التسرُّب من خلال الخطوات التالية: ..... ، ..... ، ..... .

5. من الأمور التي يجب على المنظمات مراعاتها ..... نتيجة إمكانية حدوث هجمات سلسلة التوريد؛ مما يؤدي إلى تسرُّب البيانات على نطاق واسع.

6. يمكن الاستفادة من ..... التي تساعد المنظمات في عمليات تقييم ومراقبة مخاطر الطرف الثالث.

7. من أجل الاستجابة السريعة للحوادث بهدف خفض تأثيرها على المنظمة يتطلب هذا بناء ..... لوضع خطة واضحة تحدّد الأدوار والمسؤوليات والإجراءات التي يجب اتباعها عند تسرُّب البيانات.

8. ..... هو حل أمني يعمل على تحديد والمساعدة في منع المشاركة أو النقل أو الاستخدام غير الآمن أو غير المناسب للبيانات الحساسة.

9. الحفاظ على ..... يساعد المنظمات على الالتزام بمعايير وقوانين ولوائح حماية البيانات، مع إمكانية إعداد التقارير التي تحتاجها المنظمة لإكمال عمليات التدقيق.

حلّ التمارين والتدريبات

السؤال

التمرين الأول: اختر الإجابة الصحيحة

الإجابة

1. (1)، (3) معاً.
2. جميع ما سبق.
3. جميع ما سبق.
4. فحص شبكة الويب المظلمة والعادية للعثور على تسريبات البيانات قبل استخدامها في أيّ هجوم سيبراني.

السؤال

التمرين الثاني: اكتب كلمة (صحيح) أمام العبارة الصحيحة، وكلمة (خطأ) أمام العبارة الخاطئة، وصحِّح العبارة الخاطئة

الإجابة

1. خطأ؛ يتم تسرُّب البيانات عند كشف البيانات المهمة لأشخاص غير مصرَّح لهم نتيجة حدوث أخطاء داخل المنظمة.
2. صحيح.
3. خطأ؛ إذ يكفي القيام بعملية تسريب واحدة للبيانات لتنفيذ اختراق هائل للبيانات بما يُهدّد المنظمات.
4. صحيح.
5. خطأ، بل فَقْد الأجهزة قد يُهدّد المنظمة لسهولة وصول المهاجم إلى بياناتها وخرقها.
6. خطأ، بل يُعدّ فَقْد الأجهزة بمثابة اختراق محتمل للبيانات.

7. خطأ؛ لجوء الموظفين لاستخدام الأدوات والأجهزة الشخصية، مثل الطابعات المنزلية لطباعة بيانات حساسة تخص المنظمة يُشكِّل خطراً؛ فقد يخطئ الموظف في وضع جهاز USB أو جهاز تخزين خارجي يحتوي على معلومات حساسة؛ مما يتسبَّب في سرقة الجهاز مِن قِبَل غير المصرح لهم، وتعريض المنظمة لخطر تسرُّب البيانات وهجمات الفدية وغيرها.

8. صحيح.

9. صحيح.

السؤال

التمرين الثالث: أكمل العبارات التالية

الإجابة

1. يؤدي تسرُّب البيانات إلى **سرقة الهويات سواء للموظفين أو العملاء** أو **اختراق البيانات** أو **تثبيت برمجيات ضارَّة مثل برمجية الفدية وغيرها.**

2. من أنواع البيانات المسربة في المنظمات **معلومات التعريف الشخصية، البيانات المالية، بيانات اعتماد الحساب أو تسجيل الدخول.**

3. قد تصدر خروقات البيانات عن تهديدات داخلية مرتبطة بالمنظمة، وتنقسم إلى: **الهجمات الخبيثة** وتتم بواسطة موظف غاضب من المنظمة، و**هجمات الإهمال** نتيجة كلمات المرور الضعيفة، و**حالات التوظيف** والتي تضمن قيام مجرمي الإنترنت بإغراء الموظفين داخل المنظمة لمساعدتهم على مهاجمة الشبكة وسرقة البيانات.

4. يمكن حماية بيانات المنظمات من التسرُّب من خلال الخطوات التالية: **تشفير البيانات**، **النَّسخ الاحتياطي للبيانات**، **تحديد ضوابط الوصول إلى البيانات** .

5 من الأمور التي يجب على المنظمات مراعاتها **مراقبة مخاطر الطرف الثالث** نتيجة إمكانية حدوث هجمات سلسلة التوريد؛ مما يؤدي إلى تسرُّب البيانات على نطاق واسع.

6 يمكن الاستفادة من **أدوات تقييم المخاطر** التي تساعد المنظمات في عمليات تقييم ومراقبة مخاطر الطرف الثالث.

7 من أجل الاستجابة السريعة للحوادث بهدف خفض تأثيرها على المنظمة يتطلب هذا بناء **فريق فعَّال متعدّد الوظائف يضم أعضاء من أقسام تكنولوجيا المعلومات والشؤون القانونية والعلاقات العامة والإدارات الأخرى ذات الصلة** لوضع خطة واضحة تحدّد الأدوار والمسؤوليات والإجراءات التي يجب اتباعها عند تسرُّب البيانات.

8 **منع تسرُّب البيانات** هو حل أمني يعمل على تحديد والمساعدة في منع المشاركة أو النقل أو الاستخدام غير الآمن أو غير المناسب للبيانات الحساسة.

9 الحفاظ على **الامتثال التنظيمي** يساعد المنظمات على الالتزام بمعايير وقوانين ولوائح حماية البيانات، مع إمكانية إعداد التقارير التي تحتاجها المنظمة لإكمال عمليات التدقيق.

المراجع

1. Data Breach Versus Data Leak: What's The Difference?, 2024. Follow link: https://www.teramind.co/blog/data-breach-vs-data-leak/
2. What Is a Data Leak? How They Happen and How To Prevent Them. Follow link: https://abnormalsecurity.com/glossary/data-leak
3. Data Leakage: Common Causes, Examples & Tips for Prevention. Follow link: https://www.bluevoyant.com/knowledge-center/data-leakage-common-causes-examples-tips-for-prevention
4. Over 500,000 Zoom accounts sold on hacker forums, the dark web. Follow link: https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/
5. What Is a Data Breach?. Follow link: https://www.akamai.com/glossary/what-is-a-data-breach
6. How to Detect a Data Breach (5 Critical Steps). Follow link: https://www.breachsense.com/blog/data-breach-detection/
7. Hackers targeted Twitter employees to hijack accounts of Elon Musk, Joe Biden and others in digital currency scam. Follow link: https://www.cnbc.com/2020/07/15/hackers-appear-to-target-twitter-accounts-of-elon-musk-bill-gates-others-in-digital-currency-scam.html

8. Who should encrypt the data in my company?. Follow link: https://www.sealpath.com/blog/data-encryption-for-enterprises/

9. Paul Kirvan, How can your ransomware backup strategy improve?, Feb 2020. Follow link: https://www.techtarget.com/searchdatabackup/answer/How-can-your-ransomware-backup-strategy-improve?utm_source=google&int=off&pre=off&utm_medium=cpc&utm_term=GAW&utm_content=sy_lp01252024GOOGOTHR_GsidsDataBackup_ExaGrid_Essential_IIO244839_LI2764124&utm_campaign=ExaGrid_EG_sDB_WW&Offer=sy_lp01252024GOOGOTHR_GsidsDataBackup_ExaGrid_Essential_IO244839_LI2764124&gad_source=1&gclid=EAIaIQobChMI5sep5O_lhgMVKwMGAB0gTQXxEAAYAiAAEgLR2PD_BwE

10. Kevin Mitch Group, Importance of Data Protection within the Organization, March 2023. Follow link: https://www.linkedin.com/pulse/importance-data-protection-within-organization-kevin-mitch-group/

11. How Security Leaders Can Use Multi-Factor Authentication to Protect Sensitive Data. Follow link: https://www.terranovasecurity.com/blog/multi-factor-authentication-protect-sensitive-data

12. What is Adaptive Multi-Factor Authentication (MFA)?. FOLLOW LINK: https://www.cyberark.com/what-is/adaptive-mfa/

13. Preventing and Detecting Data Leaks: The Complete Guide. Follow link: https://flare.io/learn/resources/blog/data-leakage-prevention/

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative