MSMEs

#انطلاقة_آمنة_بدايات_محصنة

المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

انطلاقة آمنة بدايات محصنة

دليل إرشادي للأمن السيبراني
لدعم المؤسسات متناهية الصغر
والصغيرة والمتوسطة في مملكة
البحرين لتعزيز المرونة السيبرانية

المحتوى

01

المقدمة

تُعد المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) ركيزة أساسية في الاقتصاد العالمي، إلا أن اعتمادها المتزايد على الأدوات الرقمية يجعلها أكثر عرضة للمخاطر السيبرانية المتزايدة. فقد صنّف المنتدى الاقتصادي العالمي (WEF) التهديدات السيبرانية ضمن أبرز المخاطر التي تواجه المؤسسات على مستوى العالم، بينما يؤكد الاتحاد الدولي للاتصالات (ITU) على أهمية ترسيخ ثقافة قوية للأمن السيبراني على مستوى العالم. ويُعد اعتماد نهج استراتيجي للأمن السيبراني أمرًا بالغ الأهمية للمؤسسات بمختلف أحجامها، سواء من خلال سياسات عالية المستوى للمؤسسات المتوسطة، أو عبر ممارسات أساسية واستعدادات بسيطة للمؤسسات المتناهية الصغر والصغيرة. ويُسهم تكييف الجهود بما يتناسب مع حجم المؤسسة وقدراتها في تعزيز مرونتها وتنافسيتها واستدامتها على المدى الطويل.

وفي إطار الجهود الوطنية لمملكة البحرين لتعزيز الجاهزية السيبرانية لدى المؤسسات المتناهية الصغر والصغيرة والمتوسطة، أطلق المركز الوطني للأمن السيبراني (NCSC) حملة "انطلاقة آمنة، بدايات محصنة" في مايو 2025، وقد تم إعداد هذا الدليل كأحد الركائز الأساسية لهذه المبادرة بهدف تمكين المؤسسات المتناهية الصغر والصغيرة والمتوسطة من حماية أصولها الرقمية من خلال إرشادات عملية واستراتيجية، ومن خلال معالجة المخاطر العالمية والاتجاهات الإقليمية والأهداف الوطنية، يُعد هذا الدليل مرجعًا موثوقًا للمؤسسات التي تعمل على بناء قواعد رقمية آمنة ومرنة في ظل اقتصاد رقمي سريع التطور.

MSMEs
#safe_start_fortified_beginnings

02

الأهمية الإستراتيجية للأمن السيبراني للمؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs)

عالميًا، تمثل المؤسسات المتناهية الصغر والصغيرة والمتوسطة أكثر من 90% من إجمالي الشركات وأكثر من 60% من فرص العمل، مما يُبرز دورها المحوري في التنمية الاقتصادية. ومع اعتماد هذه المؤسسات بشكل متزايد على التقنيات الرقمية لتعزيز قدرتها التنافسية ووصولها إلى الأسواق، فإنها تصبح أكثر عرضة للتهديدات السيبرانية.

تُظهر الدراسات الحديثة أن المؤسسات المتناهية الصغر والصغيرة والمتوسطة تواجه تحديات متزايدة في مجال الأمن السيبراني، من أبرزها:

التأثير الاقتصادي

قد تتسبب الهجمات السيبرانية في خسائر مالية كبيرة وتعطيل للعمليات وتضرر بالسمعة، وتشير التقارير إلى أن هجمات التصيد الاحتيالي تسببت في خسائر متوسطها 50 ألف دولار للمؤسسات المتضررة.

الفجوة بين التصور والواقع

كثير من المؤسسات المتناهية الصغر والصغيرة والمتوسطة تعتقد أنها "صغيرة جدًا لتكون مستهدفة"، بينما يستخدمها المهاجمون كنقطة دخول إلى شبكات أكبر.

تزايد التهديدات السيبرانية

في عام 2023 فقط، تم تسجيل أكثر من 400 مليون حالة إصابة ببرمجيات خبيثة، وكانت هذه المؤسسات من الأهداف الرئيسية بسبب محدوديات أنظمتها الأمنية.

93%

من إجمالي المؤسسات المسجلة في مملكة البحرين هي مؤسسات متناهية الصغر وصغيرة ومتوسطة (MSMEs)، مما يجعلها ركيزة أساسية في المشهد الاقتصادي للمملكة.

تُساهم هذه المؤسسات في:

- تعزيز التنوع الاقتصادي
- توفير فرص العمل
- دعم الابتكار

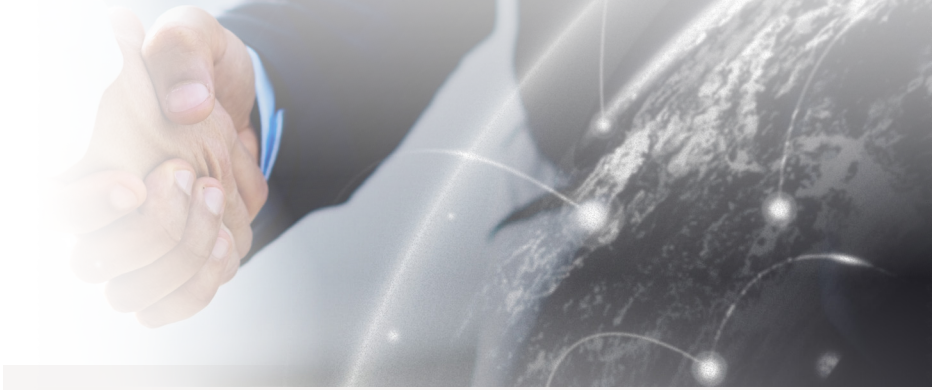
كما أن **81%** من هذه المؤسسات مملوكة لمواطنين بحرينيين، بما يقارب:

39%
يمتلكها الشباب

23%
تمتلكها النساء

مما يعكس بيئة ريادية متنوعة وحيوية.

متطلبات استراتيجية للمؤسسات المتناهية الصغر والصغيرة والمتوسطة



تبني استراتيجية متكاملة للأمن السيبراني أصبح أمرًا أساسيًا لحماية المؤسسات المتناهية الصغر والصغيرة والمتوسطة والمساهمة في استقرار الاقتصاد محليًا وعالميًا.

دمج التأمين السيبراني في استراتيجية أمن سيبراني شاملة يعزز جهود الحد من المخاطر، ويدعم استمرارية الأعمال، ويبني الثقة في الأسواق العالمية.

ومن خلال خطوات استباقية، تستطيع المؤسسات حماية أنظمتها، وبيانات عملائها، وكسب ثقة السوق الرقمي.

نظرًا **للتحديات** المتزايدة، من **المهم** أن تتبع المؤسسات نهجًا **استراتيجيًا** في **حماية** نفسها **سيبرانيًا**.

سيتناول هذا الدليل هذه النقاط بشكل عام، لمساعدة المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) على:

01

تقييم وإدارة المخاطر

02

رفع وعي الموظفين بالأمن السيبراني

03

الاستثمار في البنية التحتية الأمنية

04

التعاون لتبادل معلومات التهديدات وأفضل الممارسات

03

تطورات المشهد الأمني السيبراني عالميًا وإقليميًا

مع تزايد اعتماد المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMES)على التحول الرقمي، أصبحت هذه المؤسسات أكثر عرضة للمخاطر السيبرانية.

ويُظهر تقرير المنتدى الاقتصادي العالمي (WEF) للأمن السيبراني لعام 2025 ما يلي:

يصنف تقرير المخاطر العالمي الصادر عن المنتدى الاقتصادي العالمي (WEF) إلى أن الأمن السيبراني يُعد من أخطر التهديدات الاقتصادية.

35%

من المؤسسات الصغيرة ترى أن مستوى **مرونتها السيبرانية** في التصدي للتهديدات السيبرانية غير كافٍ، وهي نسبة ارتفعت بشكل ملحوظ مقارنة بالسنوات الماضية، مما يشير إلى تزايد نقاط الضعف في أنظمتها الأمنية.

+60%

من المؤسسات الصغيرة التي تتعرض **لهجوم سيبراني** تُغلق أبوابها خلال 6 أشهر.

10 تريليون دولار

هي التكلفة السنوية المتوقعة عالميًا **للجرائم السيبرانية** بحلول نهاية عام 2025، مما يسلّط الضوء على حجم التهديد المتزايد.

+200%

ارتفاع في هجمات **برامج الفدية** تم رصدها خلال العام الماضي، استهدفت مؤسسات على اختلاف أحجامها.

حقائق مهمة حول تطور مشهد التهديدات السيبرانية عالميًا:

80%

من هجمات **التصيد الاحتيالي** تُنفذ باستخدام تقنيات الذكاء الاصطناعي.

74%

من المؤسسات أبلغت عن تزايد **التهديدات الداخلية** خلال الفترة الأخيرة.

72.7%

من المؤسسات تتأثر **بهجمات الفدية**، التي تُعد أكبر تهديد سيبراني عالمي.

70%

من المؤسسات تتعرض لهجمات **اختراق البريد الإلكتروني التجاري (BEC)**، مما يجعلها الوسيلة الهجومية الأكثر انتشارًا.

88%

من **الحوادث السيبرانية** ناتجة عن **أخطاء بشرية**.

25%

من جميع الحوادث السيبرانية مرتبطة بـ **BEC**، مما يبرز تأثيره الكبير على مختلف القطاعات.

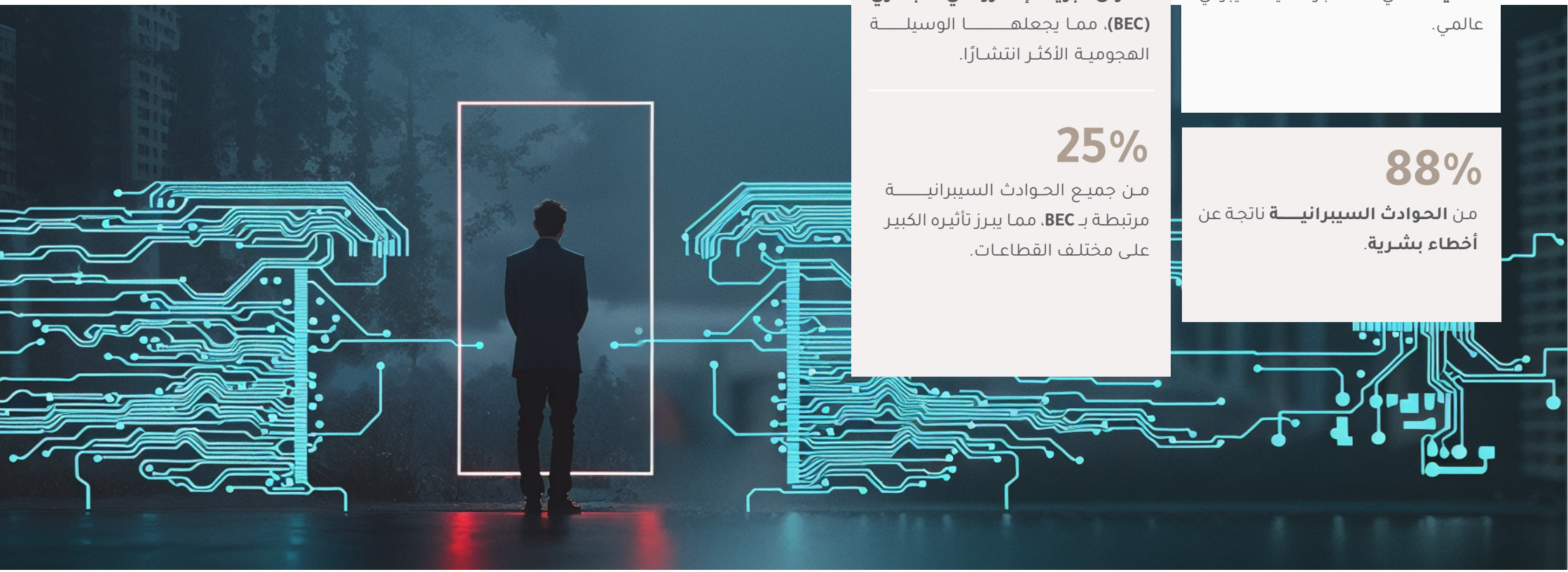
في إقليم مجلس التعاون الخليجي (GCC):

250%

ارتفعت **التهديدات السيبرانية** خلال السنوات الخمس الماضية.

استهداف القطاعات الحيوية بشكل خاص مثل **القطاع المالي والرعاية الصحية والتجارة الإلكترونية.**

ويؤكد هذا الواقع الحاجة الماسة إلى استراتيجيات شاملة للأمن السيبراني في مختلف القطاعات، ويجب على المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) أن تواكب الاستراتيجيات الوطنية للأمن السيبراني لضمان حماية عملياتها والمساهمة في استقرار الاقتصاد الإقليمي.



04

رؤيــة مملكــة البحرين الاقتصادية وجاهزيتها السيبرانيــة

تماشيًا مع رؤية مملكة البحرين الاقتصادية 2030، التي تؤكد أهمية تأمين البنية التحتية الرقمية كركيزة أساسية للتنمية الاقتصادية المستدامة، أطلق المركز الوطني للأمن السيبراني (NCSC) حملة "انطلاقة آمنة، بدايات محصنة" في مايو 2025، بهدف تعزيز الحماية السيبرانية المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs)من خلال توفير موارد توعوية وتوجيهات استراتيجية سهلة الفهم والتطبيق.

يُعد الأمن السيبراني عاملاً رئيسيًا في تمكين النمو من خلال:

جذب الاستثمارات الأجنبية وتحفيز الابتكار

حماية عمليات المؤسسات وملكيتها الفكرية

تعزيز الاقتصاد الرقمي والمالي

تؤكد رؤيــة مملكــة البحريــن الاقتصادية 2030 على أن التحول الرقمي يمثل دعامة أساسيــة للنمــو الاقتصــــــــادي.

يمنح دمج الأمن السيبراني في عمليات المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) مجموعة من المزايا الاستراتيجية، من أبرزها:

تعزيز ثقة العملاء
تُسهم حماية المعاملات والبيانات في بناء المصداقية وتعزيز ثقة العملاء.

الامتثال للأنظمة
الالتزام بالقوانين السيبرانية المحلية والعالمية يضمن التوافق القانوني ويُخفف من العقوبات المحتملة.

استمرارية الأعمال
تُسهم التدابير الاستباقية في الأمن السيبراني في الحد من توقف الأعمال الناتجة عن الحوادث السيبرانية.

القدرة التنافسية في السوق
إظهار قدرة المؤسسة على الصمود السيبراني يُعزز جاذبيتها للشركاء والمستثمرين، ويمنحها ميزة تنافسية.

يجب على المؤسسات المتناهية الصغر والصغيرة والمتوسطة دمج الأمن السيبراني في استراتيجياتها العامة لتحقيق توافق كامل مع الأهداف الاقتصادية الوطنية لمملكة البحرين، ومن خلال تبني نهج استراتيجي في الأمن السيبراني، يمكنها من:

- حماية أصولها وممتلكاتها الرقمية
- الحفاظ على ثقة عملائها
- ضمان نمو مستدام في ظل اقتصاد رقمي سريع التطور

05

كيف يدعم هذا الدليل الإرشادي جاهزية المؤسسات الصغيرة والمتوسطة في الأمن السيبراني

صُمم هذا الدليل لمساعدة المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) على فهم التحديات السيبرانية الحالية، من خلال تقديم استراتيجيات عملية وقابلة للتطوير تتماشى مع الأطر العالمية والإقليمية والوطنية للأمن السيبراني.

ومن خلال فهم المخاطر المحتملة واتخاذ إجراءات استباقية، يمكن للمؤسسات البحرينية الصغيرة والمتوسطة بمختلف أحجامها وقطاعاتها أن تعزز قدرتها على الصمود، وتحمي أصولها الرقمية، وتحافظ على ثقة العملاء، وتُسهم في بناء اقتصاد رقمي آمن ومزدهر يتماشى مع تطلعات رؤية مملكة البحرين الاقتصادية 2030.

ويُعد هذا الدليل مرجعًا موثوقًا، يقدم إرشادات سهلة الفهم تُمكن المؤسسات المتناهية الصغر والصغيرة والمتوسطة من اتخاذ خطوات استراتيجية ومدروسة لحماية عملياتها في عالم يزداد فيه الاعتماد على التكنولوجيا والاتصال الرقمي.

المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

الأمن السيبراني
عامل لدعم وتمكين
الأعمال والمشاريع

06

تصحيح المعتقدات الخاطئة عن الأمن السيبراني

تصحيح المفاهيم الخاطئة الشائعة يُعد خطوة أساسية لبناء استراتيجية أمن سيبراني فعالة، ومن خلال تصحيح هذه المعتقدات الخاطئة، يُمكن للمؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) تجنب أخطاء مكلفة وضمان استعداد أفضل للدفاع ضد التهديدات السيبرانية المتطورة. إليك بعض المعتقدات المنتشرة والحقائق التي يجب مراعاتها عند التعامل مع الأمن السيبراني.

المعتقد الأول:
بيانات المؤسسة ليست ذات قيمة لكي تستهدف

يعتقد الكثيرون أن المؤسسات الصغيرة لا تُشكل هدفًا للمهاجمين السيبرانيين، لكن الحقيقة أن كل مؤسسة مهما كان حجمها تحتفظ ببيانات ذات قيمة، مثل معلومات الدفع، وسجلات العملاء، والملكية الفكرية، وهي بيانات يمكن للمهاجمين استغلالها. غالبًا ما تُستهدف المؤسسات الصغيرة بسبب ضعف إجراءات الحماية فيها، مما يجعلها هدفًا سهلاً للهجمات السيبرانية.

المعتقد الثاني:
الأمن السيبراني مكلف جدًا على المؤسسات الصغيرة

يعتقد البعض أن الأمن السيبراني يفوق قدرة المؤسسات الصغيرة على تحمل تكاليفه، إلا أن تكلفة التعرض لهجوم سيبراني سواء من حيث الخسائر المالية أو الضرر بالسمعة، أو الغرامات قد تفوق بكثير تكلفة تطبيق تدابير الحماية الأساسية، خصوصًا أن هناك أدوات بسيطة مثل الجدار الناري، والتشفير، والمصادقة متعددة العوامل (MFA) تُعد متاحة بسهولة وتوفر حماية أساسية وفعّالة للمؤسسات.

المعتقد الثالث:
التكنولوجيا وحدها قادرة على حل مشكلات الأمن السيبراني

لا تقتصر استراتيجية الأمن السيبراني على التكنولوجيا فقط للحد من الاختراقات الأمنية، بل يُساهم الموظفون بشكل أساسي في الحد من الحوادث الأمنية، حيث تُعد الأخطاء البشرية مثل الوقوع في هجمات التصيد الاحتيالي أو فقدان الأجهزة الحلقة الأضعف في منظومة الأمن السيبراني. ويُعد النهج الشامل يجمع بين التقنيات والتدريب، ضرورة حتمية لحماية الأعمال بشكل فعال.

المعتقد الرابع:
مخاطر الأمن السيبراني تأتي فقط من مصادر خارجية

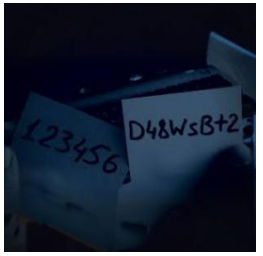
على الرغم من أن العديد من الهجمات السيبرانية تأتي من خارج المؤسسة، إلا أن التهديدات الداخلية لا تقل خطورة. فقد يتسبب الموظفون أو المتعاقدون الذين لديهم صلاحيات الوصول إلى الأنظمة الحساسة والبيانات المهمة في إحداث ضرر، سواء كان ذلك عن غير قصد أو بشكل متعمد. لذلك، من الضروري إدارة هذه المخاطر الداخلية من خلال تطبيق ضوابط وصول مناسبة، ووضع وبروتوكولات أمنية واضحة، وتدريب منتظم للموظفين.

المعتقد الخامس:
الأجهزة المحمولة آمنة من الفيروسات والبرامج الضارة والبرمجيات الخبيثة

تُعد الأجهزة المحمولة هدفًا شائعًا للمهاجمين السيبرانيين، وغالبًا ما تكون أكثر عرضة من أجهزة الحاسوب التقليدية، فهي تحتفظ بمعلومات حساسة، ويمكن أن تتعرض لخطر الاختراق بسهولة بسبب ضعف التدابير الأمنية، مثل التطبيقات غير الموثوقة أو الأجهزة المخترقة (Jailbreak)، كما أن فقدان الجهاز أو سرقته قد يؤديان إلى وصول غير مصرح به لبيانات المؤسسة.

المعتقد السادس:
برامج مكافحة الفيروسات كافية وحدها لحماية الأمن السيبراني

بالرغم أن برامج مكافحة الفيروسات تساعد في الحماية من التهديدات والاختراقات، إلا أنها لا تكفي للتصدي للهجمات السيبرانية المتقدمة مثل التصيد الاحتيالي والهندسة الاجتماعية التي يمكن أن تتجاوز تلك الحماية. لذا، فإن اتباع استراتيجية أمنية متعددة الطبقات تشمل الجدار الناري وأنظمة كشف التسلل، بالإضافة إلى تدريب الموظفين أمرًا ضروريًا لتقليل مخاطر الهجمات السيبرانية.



المعتقد السابع:
كلمات المرور القوية وحدها ستضمن بحمايتنا

تُعد كلمات المرور القوية جزءًا مهمًا من الأمن السيبراني، لكنها لا تضمن الحماية الكاملة. فالمهاجم السيبراني يمكنه اختراق كلمات المرور باستخدام أسلوب هجمات التخمين (Brute-force) أو غيرها من الأساليب. كما أن الأخطاء البشرية مثل الوقوع ضحية لرسائل التصيد الاحتيالي قد تؤدي إلى كشف كلمات المرور. لذلك، فإن استخدام المصادقة متعددة العوامل (MFA) يُضيف طبقة حماية إضافية لتعزيز أمان الوصول.

المعتقد الثامن:
التخزين السحابي آمن دائمًا

غالبًا ما يُظن أن التخزين السحابي آمن دون الحاجة إلى تدخل إضافي، لكن الواقع أن مسؤولية حماية البيانات لا تقع على مزودي الخدمة فقط، بل تشمل المؤسسات نفسها أيضًا. فقد تؤدي إعدادات سحابية غير مُحكمة أو ضعف في ضوابط الوصول إلى حدوث ثغرات أمنية، وللحفاظ على أمان البيانات في البيئة السحابية من الضروري إجراء مراجعات دورية لإعدادات الأمان، وتشفير البيانات الحساسة، وتقييد صلاحيات الوصول حسب الحاجة.

من خلال تصحيح هذه المعتقدات الخاطئة، يمكن للمؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) أن تدرك بشكل أفضل أهمية الأمن السيبراني، وتُطبق استراتيجيات فعالة لحماية أصولها الرقمية وضمان نجاح واستمرارية أعمالها.

07

أمثلة واقعية من حوادث الأمن السيبراني

مع تزايد تعقيد التهديدات السيبرانية، أصبحت حماية البيانات الحساسة ضرورة مُلِحّة لجميع أنواع الأعمال. تسلط الأمثلة التالية الضوء على دروس مهمة مستفادة من حوادث واقعية، يُمكن أن تساعد المؤسسات الصغيرة والمتوسطة (SMEs) على تعزيز أمنها السيبراني والوقاية من الهجمات الإلكترونية.

دراسة حالة
01

هجوم سيبراني تسبب في فقدان البيانات "Data-Wiping Malware"

في ديسمبر 2021، تعرضت شركة نفط كبرى في منطقة الخليج لهجوم إلكتروني باستخدام فيروس يُعرف باسم "Dustman". صُمم هذا الفيروس لمسح الملفات المهمة والتسبب في تعطل الأنظمة، مما أثر بشكل كبير على سير العمل. أظهرت التحقيقات أن الجهة المهاجمة كانت مدعومة من دولة، وقد استغلت ثغرات أمنية غير مُحدثة في شبكة الشركة.

أهم الدروس المستفادة:

1.استخدام أنظمة كشف ومنع التسلل (IDPS):
يُنصح بتركيب أنظمة لكشف التسلل على مستوى الشبكة (NIDS) وعلى مستوى الأجهزة (HIDS) لمراقبة حركة البيانات واكتشاف التهديدات بشكل مباشر ومستمر. كما يُفضل ربط هذه الأنظمة بمنصة لإدارة معلومات وأحداث الأمن السيبراني (SIEM) لتجميع السجلات وإطلاق التنبيهات بشكل تلقائي.

2. إجراء نسخ احتياطية منتظمة ووضع خطة للتعافي من الحوادث:
من المهم اتباع قاعدة النسخ الاحتياطي (3-2-1)، والتي تعتمد على الاحتفاظ بثلاث نسخ احتياطية: اثنتان على وسائط مختلفة وواحدة خارج الموقع لضمان استمرارية العمل، واحرص على تشفير النسخ الاحتياطية لحمايتها وتفعيل النسخ التلقائي لتسهيل العملية، وقُم بإجراء اختبارات دورية للتأكد من إمكانية استعادة البيانات. كما يُنصح بوضع خطة (IRP) لضمان الجاهزية الكاملة والاستجابة السريعة في حال حدوث اختراق.

دراسة حالة
02

هجوم على سلسلة التوريد في عام 2024

في عام 2024، تعرض كيان حكومي في منطقة الخليج لهجوم سيبراني متقدّم باستخدام أسلوب "هجوم سلسلة التوريد". استغل المهاجمون ثغرات في أنظمة الشركات المزودة (الطرف الثالث) لاختراق أنظمة الجهة المستهدفة، وقد أدى هذا الاختراق إلى المساس بسرية البيانات وسلامتها وتوفرها، مما تسبب في اضطرابات تشغيلية كبيرة وتهديدات مباشرة لخصوصية المواطنين.

أهم الدروس المستفادة:

1.تعزيز إدارة مخاطر الموردين:
من الضروري تطبيق برنامج لإدارة مخاطر الموردين يشمل تقييمات أمنية دورية لأنظمة الأطراف الثالثة، خاصة تلك التي تملك صلاحيات وصول للبنية التحتية الحساسة. هذا يساعد على اكتشاف الثغرات قبل أن تُستغل.

2.تطبيق ضوابط صارمة للتحكم في الوصول:
تساهم أنظمة إدارة الهوية والوصول (IAM) في تقييد الدخول إلى الأنظمة الحساسة، لضمان أن الوصول للبيانات يقتصر فقط على المستخدمين والأجهزة المصرح لهم. يُنصح بتطبيق مبدأ الحد الأدنى من الصلاحيات (PoLP)، وإجراء مراجعات صلاحيات الموردين بشكل تلقائي، وتفعيل المصادقة متعددة العوامل (MFA) لتقليل احتمالية الاختراق.

دراسة حالة
03

اختراق بيانات السحابة في عام 2019

في عام 2019، حدث اختراق كبير للبيانات في إحدى شركات التكنولوجيا المالية نتيجة لثغرة في البنية التحتية السحابية، مما أدى إلى تسريب البيانات الشخصية لأكثر من 100 مليون عميل، بما في ذلك معلومات حساسة مثل أرقام الضمان الاجتماعي، ودرجات الائتمان، وتفاصيل الحسابات البنكية.

استمر هذا الاختراق دون اكتشاف لعدة أشهر حتى قام المهاجم بالتفاخر به علنًا على الإنترنت، على الرغم من أن الشركة سارعت إلى اتخاذ إجراءات للحد من هذه الأضرار، إلا أن الحادث ألحق ضررًا كبيرًا بسمعة الشركة وأدى إلى فقدان ثقة العملاء.

أهم الدروس المستفادة:

1. تطبيق ضوابط قوية للتحكم في الوصول والصلاحيات
قم بفرض ضوابط دقيقة على البيانات الحساسة من خلال تطبيق مبدأ الحد الأدنى من الصلاحيات (PoLP)، وذلك بمنح الوصول فقط عند الضرورة.

2. مراقبة الأمان بشكل تلقائي
استخدام أدوات مؤتمتة لمراقبة البيئات السحابية باستمرار، واكتشاف الأنشطة غير المعتادة، والاستجابة السريعة للإعدادات الخاطئة أو لمحاولات الوصول غير المصرح بها.

دراسة حالة
04

اختراق بيانات بسبب ضعف أمان الشبكة الخاصة الافتراضية (VPN) وسياسة "احضر جهازك الخاص" (BYOD) في عام 2022

في عام 2022، تعرضت شركة تسويق رقمي صغيرة تفتقر إلى الموارد التقنية الكافية لخرق بيانات نتيجة ضعف أمان شبكة الافتراضية الخاصة (VPN) وسوء تطبيق سياسات "إحضار الجهاز الشخصي للعمل" (BYOD). فقد سمحت الشركة للموظفين بالوصول إلى الأنظمة عن بُعد عبر الشبكة الافتراضية الخاصة (VPN)، لكن استخدام الأجهزة الشخصية غير المؤمنة بشكل كافٍ أدى إلى خلق ثغرات كبيرة.

كما اعتمدت الشركة على بروتوكول شبكة افتراضية خاصة (VPN) قديم لم يتم تحديثه بانتظام. استغل المهاجمون هذه الثغرات، بما في ذلك جهاز موظف مخترق لا يحتوي على تحديثات مكافحة الفيروسات، ونفذوا هجوم تصيّد تمكنوا خلاله من سرقة بيانات اعتماد الشبكة الافتراضية الخاصة (VPN)، ثم الوصول إلى شبكة الشركة الداخلية وسرقة بيانات حساسة للعملاء، بما في ذلك معلومات الدفع والمراسلات التجارية.

أهم الدروس المستفادة:

1. تعزيز أمان الشبكة الافتراضية الخاصة (VPN) والمتابعة المستمرة:

يوصى بالترقية إلى بروتوكولات آمنه من الشبكة الافتراضية الخاصة (VPN) مثل OpenVPN أو IKEv2/IPSec، مع فرض المتابعة المستمرة لاكتشاف الأنشطة غير المعتادة. ويُنصح بتفعيل التنبيهات الفورية للتمكن من الاستجابة السريعة لمحاولات الوصول غير المصرح بها والحد من الهجمات التي تعتمد على سرقة بيانات الاعتماد.

2. فرض سياسة أمان قوية لاستخدام الأجهزة الشخصية (BYOD) مع تطبيق ضوابط التحكم في الوصول:

يجب فرض تشفير البيانات وضمان التحديث المنتظم للأجهزة الشخصية. كما يُمكن الاستفادة من حلول إدارة الأجهزة المحمولة (MDM) ذات التكلفة المعقولة لفرض السياسات الأمنية، وينبغي تطبيق مبدأ الحد الأدنى من الصلاحيات (PoLP) لتقييد الوصول إلى البيانات حسب الدور الوظيفي، مما يضمن أن يتمكن كل موظف من الوصول فقط إلى البيانات اللازمة لأداء عمله.

08

التهديدات السيبرانية وتقييم المخاطر للمؤسسات المتناهية الصغر والصغيرة والمتوسطة

تُستهدف المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) بشكل متزايد من قِبل المهاجمين السيبرانيين، وذلك بسبب محدودية الموارد، وضعف الاستثمار في الأمن السيبراني، والاعتماد الكبير على الأدوات الرقمية في إدارة الأعمال.

يعد فهم طبيعة التهديدات، وإجراء تقييمات منتظمة للمخاطر، من الخطوات الأساسية لبناء المرونة السيبرانية.

أبرز التهديدات السيبرانية التي تواجه المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs):

التصيد الاحتيالي والهندسة الاجتماعية

رسائل بريد إلكتروني أو رسائل مضللة تهدف إلى خداع الموظفين للكشف عن معلومات حساسة.

برامج الفدية

برمجيات خبيثة تقوم بتشفير بيانات العمل المهمة، وتطلب مبلغًا ماليًا مقابل فك التشفير.

التهديدات الداخلية

مخاطر ناتجة عن موظف حالي أو سابق، أو مورد خارجي لديه صلاحية الوصول إلى الأنظمة.

تسرب البيانات

وصول غير مصرح به يؤدي إلى سرقة أو كشف بيانات العملاء أو بيانات العمل.

هجمات سلسلة التوريد

استغلال الثغرات لدى الموردين أو مقدمي الخدمات لاختراق أنظمة المؤسسات.

هجمات حجب الخدمة (DoS)

تعطيل أنظمة أو مواقع المؤسسة من خلال إرسال عدد هائل من الطلبات بهدف إيقافها عن العمل.

أهمية تقييم المخاطر

يساهم التقييم الدوري للمخاطر السيبرانية في مساعدة المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) على:

- تحديد الأصول الرقمية والمادية الهامة وترتيبها حسب الأولوية.
- تطبيق استراتيجيات فعالة لتقليل المخاطر.
- التعرف على نقاط الضعف والطرق التي قد يستخدمها المهاجمون.
- التركيز على استخدام الموارد لحماية أكثر الأمور خطورة أولاً.

نهج عملي لتقييم المخاطر للمؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMES)

يمكن للمؤسسات المتناهية الصغر والصغيرة والمتوسطة اتباع نهج مبسط وفعال لتقييم المخاطر السيبرانية:

1. تحديد الأصول

حصر الأصول الرقمية والمادية مثل الخوادم وبيانات العملاء والملكية الفكرية.

2. تحديد التهديدات ونقاط الضعف

فهم كيفية تعرض الأصول للتهديد وما هي الثغرات الموجودة.

3. تقدير أثر التهديد واحتمالية حدوثه

فهم الأثر المحتمل لكل تهديد على العمل ومدى احتمال وقوعه.

4. ترتيب المخاطر حسب الأولوية

الاهتمام أولاً بالنقاط التي تواجه أعلى مستوى من الخطر.

5. تنفيذ ضوابط الحماية

تطبيق الضوابط المناسبة وفقًا لمتطلبات الأمن السيبراني واتخاذ تدابير الوقاية اللازمة.

6. المراقبة والمراجعة

مراجعة ملف المخاطر بشكل دوري وتحديث الاستراتيجية حسب تطور التهديدات.

نصيحة:

يمكن للمؤسسات المتناهية الصغر والصغيرة والمتوسطة الاستفادة من الأطر الدولية مثل إطار الأمن السيبراني (NIST) الصادر عن المعهد الوطني للمعايير والتقنية أو معيار (ISO/IEC27005) كدليل، وتطبيقها بشكل مبسط يتناسب مع حجم أعمالهم.

09

مستويات الجاهزية السيبرانية للمؤسسات المتناهيـــة الصغر والصغيرة والمتوسطة (MSMEs)

بناء القدرات في الأمن السيبراني ليس خطوة تُنفذ مرة واحدة، بل هو مسار مستمر من التطوير والتحسين. ولمساعدة المؤسسات على التدرج في تحسين حمايتها الرقمية، يقدم هذا النموذج ثلاث مراحل عملية لتطوير الجاهزية السيبرانية.

حيث يتيح كل مستوى للمؤسسات بمختلف أحجامها وإمكاناتها تطبيق ممارسات تتناسب مع احتياجاتها التشغيلية ومواردها.

المستوى 1

الممارسات الأساسية (Cyber Hygiene)

وجود حماية أساسية في المؤسسة مع التركيز على التعامل مع التهديدات بعد حدوثها، دون استعداد استباقي.

الإجراءات الرئيسية

- تثبيت برامج مكافحة الفيروسات والجدران النارية.
- إجراء نسخ احتياطية منتظمة للبيانات.
- تفعيل المصادقة متعددة العوامل (MFA).
- تدريب أساسي للموظفين في مجال الأمن السيبراني.

المستوى 2

إدارة الأمن السيبراني

إدارة استباقية للتهديدات من خلال إجراءات موثقة ومراجعات دورية.

الإجراءات الرئيسية

- وضع سياسات وإجراءات للأمن السيبراني.
- إعداد تقييم للمخاطر وخطط للاستجابة عند وقوع الحوادث السيبرانية.
- تنفيذ فحص دوري للثغرات.
- تدريب الموظفين على التهديدات المتقدمة، مثل رسائل التصيد الوهمية.

المستوى 3

الجاهزية السيبرانية المتقدمة

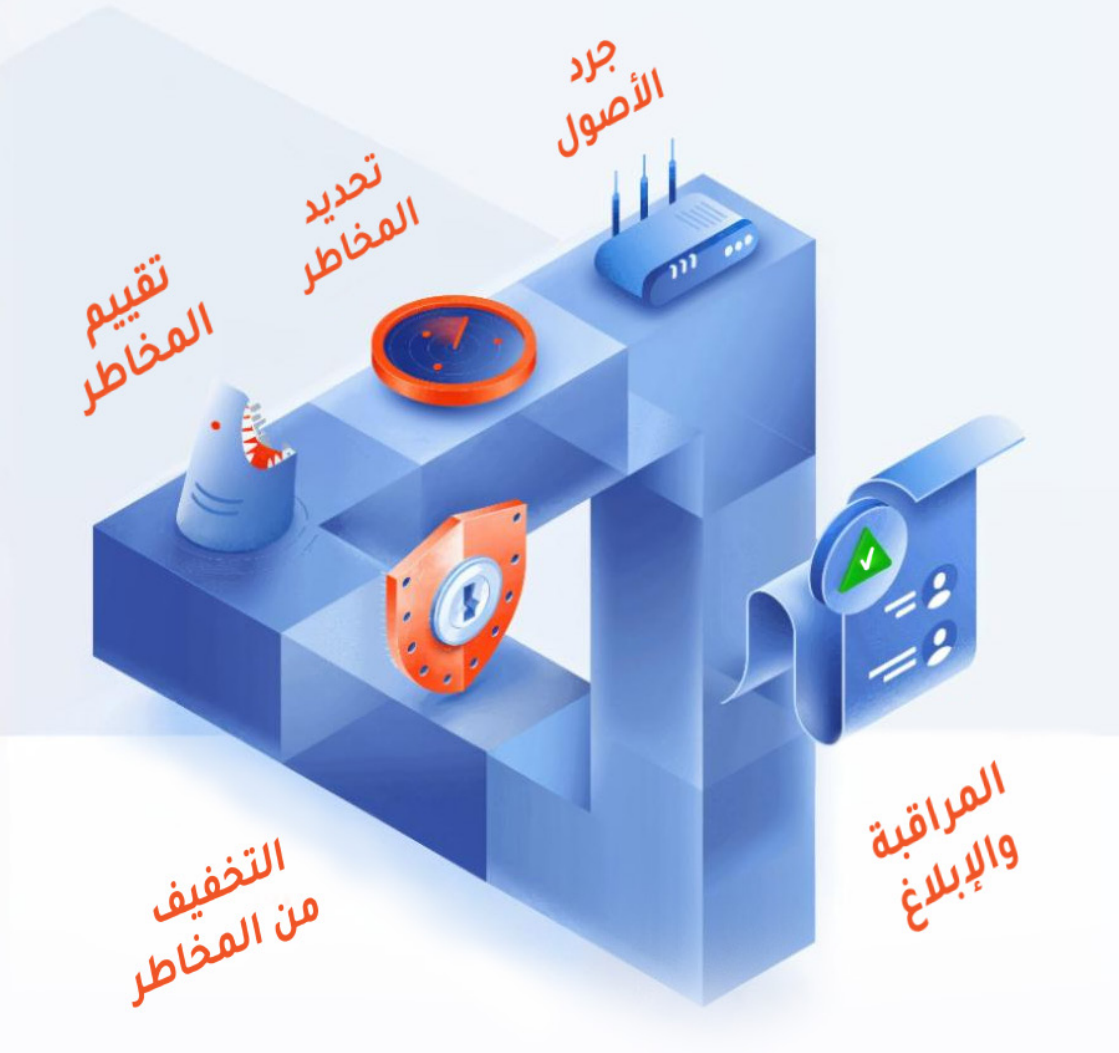
دمج الأمن السيبراني ضمن ثقافة واستراتيجية المؤسسة. والتحسين المستمر بقيادة الإدارة.

الإجراءات الرئيسية

- دمج الأمن السيبراني في جميع تطبيقات التكنولوجيا "التصميم الآمن"
- التعاون مع شبكات متخصصة لتبادل معلومات التهديدات السيبرانية.
- التحقق من قوة الحماية عبر اختبارات أمنية منتظمة.
- تعيين مسؤول مختص بالأمن السيبراني أو الاستعانة بجهة خارجية.

ملاحظة:

ينبغي على المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs) أن تسعى للتقدم التدريجي عبر هذه المراحل بما يتناسب مع مواردها، ومستوى استعدادها لتحمل المخاطر، واحتياجات نشاطها التجاري. فالوصول إلى المستوى الثاني وحده يُعد خطوة كبيرة تعزز بشكل كبير قدرتها على التصدي لمعظم التهديدات السيبرانية الشائعة.



10

إطار SMESEC:
10 خطوات استراتيجية لتعزيز الأمن السيبراني للمؤسسات الصغيرة والمتوسطة

01 بناء قيادة واضحة وإدارة فعالة للمخاطر السيبرانية

- دعم الأمن السيبراني من أعلى مستويات الإدارة.
- وضع سياسة شاملة لإدارة مخاطر الأمن السيبراني.
- إجراء تقييمات دورية للمخاطر وتحديد الإجراءات المناسبة للحد منها.

02 تعزيز ضوابط الوصول ووسائل التحقق

- تطبيق مبدأ الحد الأدنى من الصلاحيات (PoLP) للوصول من قبل المستخدمين.
- فرض المصادقة متعددة العوامل (MFA) للأنظمة الحساسة.
- مراجعة صلاحيات الوصول بانتظام.

03 حماية الأنظمة والتطبيقات

- التأكد من أن جميع الأجهزة والبرامج محدثة بأحدث الإصدارات.
- تثبيت برامج مكافحة الفيروسات وحماية نقاط النهاية.
- إزالة أو تعطيل الخدمات غير الضرورية.

04 الحماية من البرامج الخبيثة وهجمات التصيد الاحتيالي

- تدريب الموظفين على التعرف على رسائل التصيد الاحتيالي والإبلاغ عنها.
- استخدام خاصية تصفية رسائل البريد الإلكتروني الضارة.
- تثبيت برامج الحماية من البرمجيات الخبيثة على جميع الأجهزة.

05 حماية البنية التحتية للشبكة

- تطبيق او تفعيل جدران نارية وأنظمة كشف التسلل (IDS).
- استخدام الشبكات الافتراضية الخاصة (VPNs) للوصول عن بُعد.
- تقسيم الشبكة لعزل الأصول الحساسة.

06 النسخ الاحتياطي وتأمين البيانات

- إجراء نسخ احتياطية منتظمة وآلية.
- تشفير بيانات النسخ الاحتياطي وتخزينها بأمان في مواقع خارجية.
- إجراء اختبارات دورية لاستعادة النسخ الاحتياطي.

07 إعداد واختبار خطة استجابة للحوادث الأمنية (IRP)

- إعداد خطة استجابة تتناسب مع حجم عملك.
- تحديد إجراءات التواصل في حالات الحوادث.
- إجراء تدريبات دورية للتحقق من الجاهزية لمواجهة الحوادث.

08 تعزيز ثقافة الوعي بالأمن السيبراني

- إجراء تدريبات منتظمة لزيادة الوعي بالأمن السيبراني.
- إعلام الموظفين حول التهديدات الجديدة وطرق الوقاية منها.
- تشجيع الإبلاغ عن أي نشاط مشبوه.

09 تأمين سلسلة التوريد

- تقييم ممارسات الأمن السيبراني لدى الموردين الرئيسيين.
- التأكد من تضمين متطلبات الأمن السيبراني في العقود.
- مراقبة شركاء سلسلة التوريد بشكل مستمر لرصد المخاطر.

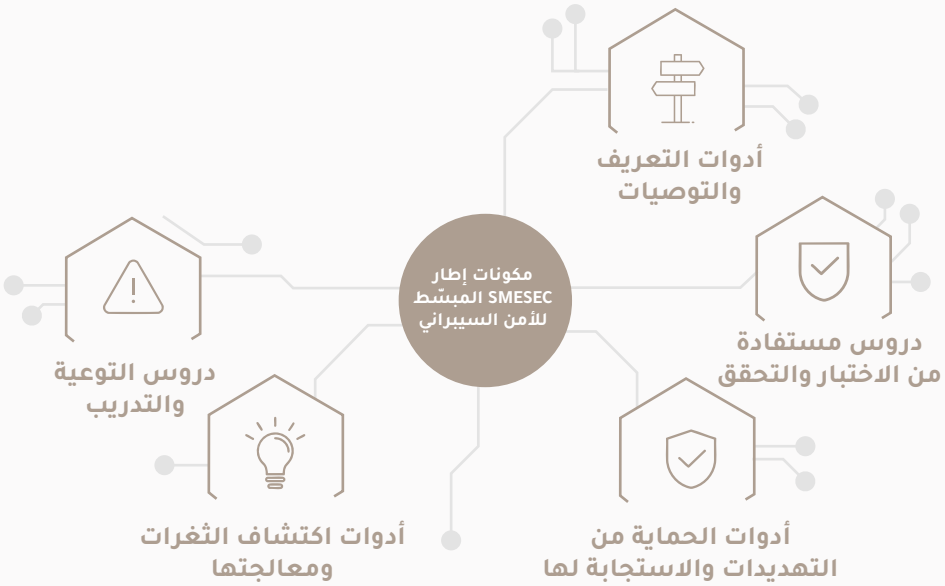
10 التدقيق والتحسين

- مراقبة أنظمة تقنية المعلومات بشكل مستمر لرصد التهديدات.
- إجراء مراجعات أمنية بشكل دوري.
- تحديث السياسات والضوابط عند ظهور تهديدات جديدة.

إطار عمل SMESEC

يشير SMESEC إلى "أمن المؤسسات الصغيرة والمتوسطة" (Small and Medium Enterprise Security)، وهو إطار مبسّط وفعّال للأمن السيبراني، يهدف إلى حماية المؤسسات الصغيرة والمتوسطة من التهديدات السيبرانية.

يُتيح هذا الإطار لأصحاب تلك المؤسسات تحديد الثغرات الأمنية والتعامل معها بأنفسهم من خلال أدوات تعليمية بسيطة، ودروس تدريبية، وتجارب عملية مستفادة.



11

أفضل الممارسات العالمية للأمن السيبراني للمؤسسات المتناهية الصغر والصغيرة والمتوسطة

يوضح الجدول التالي كيف تتماشى الأطر الدولية الرئيسية للأمن السيبراني مع دعم المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs):

الركائز الأساسية	الإطار	الركائز الأساسية	الإطار
01 **دليل المرونة السيبرانية من المنتدى الاقتصادي العالمي - WEF**	o تعزيز ثقافة إدارة المخاطر o بناء المرونة في سلاسل التوريد	03 **ركن الأمن السيبراني للمؤسسات الصغيرة من المعهد الوطني للمعايير والتقنية - NIST**	o التركيز على الوظائف الخمس للأمن السيبراني: التعرف، الحماية، الاكتشاف، الاستجابة، والتعافي. o تقديم قوائم تحقق مخصصة للأمن السيبراني للمؤسسات الصغيرة والمتوسطة (SMEs)
02 **إطار الأساسيات السيبرانية من المركز الوطني للأمن السيبراني في المملكة المتحدة - UK NCSC**	o تأمين الاتصال بالإنترنت o تأمين الأجهزة والبرمجيات o التحكم في الوصول إلى البيانات والخدمات o الحماية من الفيروسات والبرمجيات الخبيثة o تحديث البرمجيات بانتظام	04 **أجندة الأمن السيبراني العالمية من الاتحاد الدولي للاتصالات - ITU**	o تطوير الأطر القانونية والتنظيمية o تعزيز الهياكل التنظيمية o بناء التعاون على المستويين الوطني والدولي

12

في الختام،
"قم بتمكين رحلتك في مجال الأمن السيبراني"

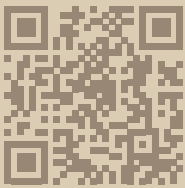
تلعب المؤسسات المتناهية الصغر والصغيرة والمتوسطة (MSMEs)، دورًا حيويًا في نمو الاقتصاد البحريني وابتكاره. ومع تزايد اعتمادها على التقنيات الرقمية، أصبح تعزيز ممارسات الأمن السيبراني أمرًا أساسيًا لحماية عملياتها، وثقة العملاء، وضمان نجاحها على المدى الطويل.

يُقدم هذا الدليل إرشادات استراتيجية مصممة خصيصًا لتعزيز مرونة هذه المؤسسات في مجال الأمن السيبراني، بما يتماشى مع رؤية مملكة البحرين الاقتصادية 2030 وأفضل الممارسات العالمية.

يُعد الأمن السيبراني الفعال نتيجة للتعاون الجماعي وليس للجهود المنفردة. لذا، يُنصح بأن تتعاون هذه المؤسسات مع السلطات المعنية والجهات الوطنية والقطاعية المختصة مثل المركز الوطني للأمن السيبراني (NCSC)، وفي حال حدوث حادث سيبراني فالإبلاغ السريع إلى هذه الجهات ستوفر الاستجابة السريعة والدعم الفني المتخصص، مما يعزز آليات الدفاع الجماعي.

من خلال اعتماد نهج استباقي في الأمن السيبراني والتعاون مع الموارد الوطنية الموثوقة، لا تُسهم هذه المؤسسات في تعزيز مرونتها التجارية فحسب، بل أيضًا في دعم المنظومة الشاملة للأمن الرقمي في مملكة البحرين.

ابقَ **آمنًا.**
ابقَ **مرنًا.**



ncscbh

ncsc_bh

www.ncsc.gov.bh