الدورة التدريبية: الأمن الشامل للشركات الصغيرة والمتوسطة: حلول فعالة ومنخفضة التكلفة



19 - 23 اكتوبر 2026
القاهرة
3700 € (للشخص الواحد)
Ref: #SM1741_424529

مقدمة الدورة التدريبية / لمحة عامة:

تواجه الشركات الصغيرة والمتوسطة (SMBs) تحديات أمنية متزايدة ومعقدة، غالبًا ما تكون ذات موارد محدودة للتعامل معها. فالهجمات السيبرانية لا تستهدف الشركات الكبيرة فحسب، بل أصبحت الشركات الصغيرة والمتوسطة هدفًا رئيسيًا للمخترقين نظرًا لضعف دفاعاتها غالبًا. تهدف هذه الدورة التدريبية المتخصصة، التي يقدمها BIG BEN Training Center، إلى تزويد أصحاب الأعمال والمديرين والموظفين في الشركات الصغيرة والمتوسطة بالمعرفة والمهارات اللازمة لتطبيق حلول أمنية فعالة ومنخفضة التكلفة لحماية أصولهم وبياناتهم. ستغطي الدورة الجوانب الأساسية للأمن السيبراني، وأمن البيانات، والأمن المادي، مع التركيز على الاستراتيجيات العملية التي يمكن تطبيقها بموارد محدودة. تستند هذه الدورة إلى أحدث الإرشادات وأفضل الممارسات الأمنية المصممة خصيصًا للشركات الصغيرة والمتوسطة، مستلهمة من أعمال أكاديميين بارزين مثل البروفيسور Scott Shackelford (سكوت شاكلفورد)، الذي ركزت أبحاثه على الأمن السيبراني والاقتصاد الرقمي، وقدم رؤى حول كيفية بناء المرونة السيبرانية للمؤسسات بغض النظر عن حجمها. تهدف الدورة إلى تمكين الشركات الصغيرة والمتوسطة من حماية نفسها من التهديدات، والحفاظ على استمرارية أعمالها، وبناء ثقة العملاء في بيئة رقمية متزايدة الخطورة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- أصحاب الشركات الصغيرة والمتوسطة.
- المدراء التنفيذيون في الشركات الصغيرة والمتوسطة.
- مدراء تكنولوجيا المعلومات في الشركات الصغيرة والمتوسطة.
- الموظفون المسؤولون عن أمن البيانات والأنظمة.
- مدراء الموارد البشرية (فيما يتعلق بوعي الموظفين).
- رواد الأعمال والشركات الناشئة.
- أي موظف يرغب في تعزيز فهمه للأمن المؤسسي.
- المستشارون الذين يخدمون الشركات الصغيرة والمتوسطة.

القطاعات والصناعات المستهدفة:

- شركات الخدمات المهنية (قانونية، محاسبية، استشارية).
- شركات التجزئة والتجارة الإلكترونية الصغيرة.
- شركات تكنولوجيا المعلومات والبرمجيات الصغيرة.
- العيادات الطبية والمنشآت الصحية الصغيرة.
- شركات الضيافة والسياحة الصغيرة.
- الشركات الصناعية والإنتاجية الصغيرة.
- المؤسسات التعليمية الصغيرة.
- الهيئات الحكومية المحلية والبلديات.

الأقسام المؤسسية المستهدفة:

- الإدارة العليا.
- قسم تكنولوجيا المعلومات (إن وجد).
- القسم المالي.
- قسم العمليات.
- قسم الموارد البشرية.
- قسم خدمة العملاء.
- المبيعات والتسويق.
- جميع الموظفين بشكل عام.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم أساسيات الأمن السيبراني والمخاطر الشائعة للشركات الصغيرة والمتوسطة.
- تطبيق إجراءات أمنية بسيطة وفعالة لحماية البيانات.
- تأمين الشبكات والأنظمة الأساسية بميزانية محدودة.
- تطوير خطة استجابة للحوادث الأمنية.
- تثقيف الموظفين حول أفضل ممارسات الأمن السيبراني.
- اختيار وتنفيذ حلول أمنية منخفضة التكلفة ومفتوحة المصدر.
- حماية معلومات العملاء والامتثال للوائح الخصوصية.
- إدارة النسخ الاحتياطي واستعادة البيانات.
- تأمين البريد الإلكتروني والاتصالات الرقمية.
- بناء ثقافة أمنية مستدامة داخل المؤسسة.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة منهجية تدريبية عملية وتطبيقية، مصممة خصيصًا لتلبية احتياجات الشركات الصغيرة والمتوسطة التي تتطلب حلولًا أمنية فعالة بأقل التكاليف. ستتضمن المنهجية محاضرات تفاعلية تستعرض التهديدات الأمنية الأكثر شيوعًا التي تواجه الشركات الصغيرة والمتوسطة، وأساليب الاختراق الحديثة. سيتم التركيز على دراسات الحالة الواقعية لشركات صغيرة ومتوسطة تعرضت لهجمات، مع تحليل الأسباب وكيفية تجنبها. سيشارك المتدربون في ورش عمل تطبيقية تركز على تنفيذ حلول أمنية مجانية أو منخفضة التكلفة، مثل تكوين جدران الحماية، وإعداد النسخ الاحتياطي الآمن، وتدريب الموظفين على اكتشاف رسائل التصيد الاحتيالي. تهدف هذه المنهجية إلى تزويد المشاركين بالمعرفة والمهارات العملية اللازمة لتعزيز الوضع الأمني لشركاتهم، مع التركيز على الحلول التي يمكن تطبيقها بسهولة وبتكلفة معقولة.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: فهم التهديدات الأمنية للشركات الصغيرة والمتوسطة

- أهمية الأمن السيبراني للشركات الصغيرة والمتوسطة.
- التهديدات الشائعة (التصيد الاحتيالي، البرمجيات الخبيثة، هجمات الفدية).
- نقاط الضعف الفريدة في الشركات الصغيرة والمتوسطة.
- الفرق بين الأمن السيبراني والأمن المادي.
- أهمية النسخ الاحتياطي للبيانات.
- مخاطر فقدان البيانات والسمعة.
- تأثير الهجمات السيبرانية على استمرارية الأعمال.

الوحدة الثانية: أساسيات حماية الشبكات والأنظمة

- تأمين الشبكات اللاسلكية (Wi-Fi).
- إعدادات جدار الحماية (Firewall) الأساسية.
- حماية أجهزة الكمبيوتر والمخدمات.
- تحديث البرامج والأنظمة بانتظام.
- استخدام برامج مكافحة الفيروسات والبرمجيات الضارة.
- أمن الأجهزة المحمولة للموظفين.
- أمن الأجهزة المتصلة بالإنترنت (IoT).

الوحدة الثالثة: تأمين البيانات والتحكم في الوصول

- تصنيف البيانات وتحديد البيانات الحساسة.
- سياسات كلمات المرور القوية وإدارة الهوية.
- التحكم في الوصول إلى الملفات والمجلدات.
- تشفير البيانات الحساسة.
- حلول التخزين السحابي الآمن.
- أمن البريد الإلكتروني (Email Security).
- التعامل الآمن مع بيانات العملاء.

الوحدة الرابعة: تدريب الموظفين والاستجابة للحوادث

- أهمية الوعي الأمني للموظفين.
- تدريب الموظفين على اكتشاف هجمات التصيد الاحتيالي.
- سياسات الاستخدام المقبول للموارد التقنية.
- تطوير خطة بسيطة للاستجابة للحوادث الأمنية.
- الخطوات الأولى عند وقوع حادث أمني.
- أهمية الإبلاغ عن الحوادث الأمنية.
- التعاون مع خبراء الأمن عند الحاجة.

الوحدة الخامسة: أدوات وحلول أمنية منخفضة التكلفة والاستمرارية

- أدوات أمنية مجانية ومفتوحة المصدر.
- خدمات الأمن المدارة للشركات الصغيرة والمتوسطة.
- أمن النسخ الاحتياطي واستعادة البيانات.
- خطط استمرارية الأعمال والتعافي من الكوارث.
- تأمين التعاملات المالية عبر الإنترنت.
- أهمية التقييم الدوري للوضع الأمني.
- بناء برنامج أمني مستمر ومناسب للميزانية.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

في ظل الموارد المحدودة والتهديدات السيبرانية المتزايدة، كيف يمكن للشركات الصغيرة والمتوسطة أن تتبنى استراتيجيات أمنية مرنة ومستدامة، تضمن حماية أصولها الحيوية وبيانات عملائها، دون أن تثقل كاهلها بتكاليف باهظة أو تعرقل نموها؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بتركيزها العملي والموجه خصيصًا لاحتياجات الشركات الصغيرة والمتوسطة، حيث تقدم حلولًا أمنية فعالة ومناسبة للميزانية، بعيدًا عن التعقيدات التقنية غير الضرورية. يقدم BIG BEN Training Center محتوى أكاديميًا وعمليًا، يستند إلى أفضل الممارسات الأمنية التي يمكن تطبيقها بسهولة في بيئات الشركات الصغيرة. ما يميز هذه الدورة هو تركيزها على الجوانب التطبيقية من خلال ورش العمل التفاعلية والأمثلة الواقعية، التي تمكن المتدربين من تنفيذ إجراءات أمنية ملموسة بأنفسهم. بدلاً من مجرد سرد الأدوات، توفر الدورة رؤى حول كيفية بناء ثقافة أمنية، وتدريب الموظفين، والاستجابة للحوادث بفعالية، مما يجعلها ضرورية لأي شركة صغيرة ومتوسطة تسعى لتعزيز دفاعاتها ضد التهديدات الرقمية المتزايدة.