SANS SECURITY AWARENESS

دليل خطّة العمل الطارئة للوعي الأمني – تأمين العمل من المنزل

ملخّص تنفيذي

بسبب إنتشار فيروس كورونا، وجّهت منظّمات كثيرة موظّفيها للعمل من منازلهم. إنّ هذا تحدٍ كبير لأنّ أكثر المنظمّات لم تُجهّز سياسات أو تقنيات أو التدريب الضروري لتأمين عمل الموظّفين من منازلهم. إضافة إلى هذا، قد يجد كثير من الموظّفين أنفسهم بحالة غير مألوفة لهم أو غير مريحة حين يتعلّق الأمر بالعمل من المنزل. هدف هذا الدليل الإرشادي هو مساعدتك على تدريب هؤلاء الأفراد ليكونوا على أفضل مستوى أمني ممكن وبسرعة. تواصل معنا بواسطة عنوان البريد الإلكتروني هذا support@sans.org إذا كانت لديك أيّ أسئلة عن أيّ فقرة في هذا الدليل الإرشادي.

لأنّ فريق عملك يمرّ بتغيير كبير يُرافقه قدر كبير من التوتّر، ولأنّ منظمتك مقيّدة بفترة زمنية وموارد مُحدّدة، فإنّ هذا الدليل الإستراتيجي يُركّز على تسهيل مفهوم التدريب. ننصحك بالتركيز فقط على أهمّ المخاطر المُفضّلة أدناه التي يكون لها أكبر تأثير عليك. فكّر بها على أنّها نقطة البداية. إذا كانت هناك مخاطر أو مواضيع أخرى تريد إضافتها فلك الحرّية بذلك. لكن عليك أنّ تُدرك أنّه كلما زادت السلوكيات والإجراءات أو التقنيات المطلوبة من فريق عملك، قلّ احتمال إمكانية تطبيقها كلّها.

كيف تستخدم هذا الدليل الإرشادي

ننصحك أوّلًا قراءة هذا الدليل الإرشادي وزيارة الروابط الإلكترونية التي ستوجّهك إلى مواد متعدّدة تعطيك فكرة واضحة عمّا وفّرناه لك. سترى أنّنا قدّمنا لك مجموعة متنوّعة من المواد الخاصّة بكل نوع من المخاطر حتى تستخدمها في تفاعلك وتدريبك أفراد منظمّتك. ستستطيع من خلال هذه الموارد اختيار المواد التي تراها أكثر فاعلية والمناسبة لاحتياجاتك وثقافة منظمتك. بعد إنهاء قراءة هذه الوثيقة، إقرأ وثيقة النموذج الإعلامي وورقة المعلومات المرفقتين في هذا الملف حتى تفهم بطريقة أفضل الهدف الذي تُحاول تحقيقه. بعد قراءتك للوثائق الثلاثة سيكون عليك التنسيق مع مجموعتين أساسيتين.

1. **فريق الأمن:** نسّق جهودك مع فريق الأمن لتحصل على فهم أفضل عن المخاطر التي عليك التعامل معها وإدارتها. حدّدنا في هذا الدليل الإرشادي مجموعة نراها على أنّها أهمّ المخاطر وأكثرها شيوعًا التي تُهدّد فرق العمل العاملة من المنازل، لكنّ المخاطر التي تهمّك قد تكون مختلفة. تنبيه: من الأخطاء الشائعة لفرق الأمن أنّها تُحاول إدارة كلّ المخاطر وتُغرق الموظفّين بعدد كبير من السياسات والمتطلّبات العاجلة. لذا، حاول الحدّ حتى أقلّ عدد ممكن من المخاطر التي تُريد التكلّم عنها ومعالجتها. بعد تحديدك أنواع هذه المخاطر وترتيب أولوياتها، حدّد السلوكيات المطلوبة لإدارة هذه المخاطر. مثلما ذكرنا سابقًا، إذا لم يكن لدى منظمتك الوقت والموارد الضرورية لهذا، عليك التركيز واغتنام التوجيهات التي سنذكرها أدناه.
2. **فريق الإعلام والتواصل:** بعد تحديدك أهمّ المخاطر البشرية والسلوكيات الأساسية لإدارة هذه المخاطر، عليك التشارك مع فريق الإعلام في منظمتك للتفاعل وتدريب فريق عملك على هذه السلوكيات الجديدة. لهذا نجد أنّ أكثر برامج الوعي الأمني فاعلية هي تلك المبنية على تشارك متين مع فريق الإعلام والتواصل. حاول ضمّ فرد من فريق الإعلام إلى فريقك الأمني إذا كان هذا ممكنًا. من الطرق المناسبة لجعل فرق عملك تتفاعل إيجابيًا وسريعًا عند التواصل الإعلامي معهم التركيز على أنّ هذا التدريب سيؤمنّهم أثناء عملهم وسيجعل أيضًا من منازلهم آمنة إلكترونيًا لحماية أنفسهم وعائلاتهم.

وبالعمل مع هاتين المجموعتين ستُحاول جعل الأمن بسيطًا قدر الإمكان على فرق العمل وتوفّر لهم التحفيز الضروري، وهذان عاملان أساسيان للتغيير السلوكي. نقترح عليك أيضًا تشكيل مجلس إستشاري يجمع إختصاصيين تحتاج لآرائهم وتقييماتهم حتى تنجح في إطلاق هذا البرنامج. إلى جانب فريق الأمن وفريق الإعلام والتواصل، قد ترغب بالتعاون مع أقسام أخرى مثل قسم الموارد البشرية والقسم القانوني.

رزمة التنزيل الرقمي MGT443

يُوفّر معهد SANS Institute دورة تدريبية تستمر يومين عنوانها: MGT433: كيفية صناعة وصيانة وقياس برنامج وعي أمني عالي المستوى والتأثير. توفّر هذه الدورة المُكثّفة كلّ النظريات الأساسية والمهارات وأطر العمل والموارد الضروريّة لبناء برنامج وعي أمنيّ عالي المستوى والتأثير لمساعدتك على قياس عوامل المخاطر البشرية والتعامل الفاعل معها. ضمن هذا الدليل الإرشادي سنُقدّم لك مجّانًا رزمة التنزيل الرقمية الخاصة بالدورة التدريبية والتي تشمل نماذج أساسية وموارد تخطيطية. ومع أنّ هذه المواد ستزيد متطلّبات هذه المبادرة، إلّا أنّ هذه المواد ستكون ذات قيمة عالية للمنظّمات الكبيرة أوالتي تريد إنفاذ عمليات طوارئ أكثر تطوّرًا وتعقيدًا.

الإجابة على أسئلة فرق العمل

إضافة لنشر المذكور أعلاه، ننصحك باستخدام نوع من التقنيات أو منتدى عام للإجابة عن أسئلة الناس ويُفضّل فعل هذا بطريقة سريعة ومباشرة. يُمكن أن يشمل هذا وسائل مُخصّصة لهذا الهدف مثل عناوين بريد إلكترونية أو حسابًا على سكايب (Skype) أو قنوات دردشة من برنامج سلاك (Slack) أو منتدى عام إلكتروني مثل منتدى يامر (Yammer). من الأفكار الأخرى إستضافة جلسة أمنية منقولة بواسطة الإنترنت تُحدّد لها عدّة مواعيد أسبوعيًا حتى يختار الناس الوقت الذي يناسبهم ويحضروا الجلسة مباشرة ويُمكنهم أيضًا طرح الأسئلة أيضًا. الهدف من هذا جعل موضوع الأمن قريبًا من الناس ومساعدتهم في الإجابة عن أسئلتهم. هذه فرصة مناسبة للتفاعل مع الموظّفين وإظهار موضوع الأمن بطريقة لطيفة، لذا حاول إغتنام هذه الفرصة. تذكّر أنّه لإنجاز هذا الأمر بفاعلية، عليك تعيين موظّف خاصّ لإدارة هذه القنوات و/أو الإجابة عن الأسئلة بطريقة سريعة ونشطة.

مواد التدريب والمخاطر

لقد حدّدنا ثلاثة مخاطر أساسية عليك إدارتها لأفراد فرق العمل عن بعد. هذه نقاط بداية ويُرجّح أنّها ستكون ذات الأهمية القصوى لك. ستجد لكلّ خطر مذكور أدناه روابط إلى عدّة موارد مهمّة تُساعدك على التواصل الإعلامي وإجراء التدريبات المرتبطة بالموضوع. لقد وفّرنا لك عدّة مواد إعلامية تواصلية حتى تختار منها تلك التي لها أكبر تأثير على ثقافتك. إضافة إلى هذا ستجد أنّ أكثر هذه المواد متوافرة بلغات متعدّدة. إذا كانت هذه الأمور كثيرة عليك ووقتك محدودٌ جدًّا، ننصحك باستخدام المادتين أدناه.

1. ورقة الحقائق للعمل الآمن من المنزل (مُرفقة مع ملف خطّة العمل الطارئة).
2. الشريط المرئي بعنوان: البيت الآمن إلكترونيًا (بالإنكليزية) متوافر أيضًا بلغات أخرى هنا

الهندسة الاجتماعية

تُعتبر هجمات الهندسة الاجتماعية واحدة من أشدّ المخاطر التي يواجهها العاملون عن بعد، خصوصًا في هذا الوقت الذي نشهد فيه تغيرًا سريعًا في بيئة طارئة. الهندسة الاجتماعية هي هجمة ترتكز على العامل النفسي حيث يُحاول المهاجم خداع ضحاياه ودفعهم لارتكاب خطأ، وعلينا معرفة أنّ هذا الأمر سيسهل على المهاجم في أوقات التغيير والارتباك. مفتاح المواجهة هو تدريب الافراد على معرفة الهندسة الاجتماعية وكيفية رصد أهمّ المؤشّرات الدالّة عليها ثمّ ما يجب عليهم فعله بعد رصد تلك الهجمات. لا تركّز على هجمات التصيّد بواسطة رسائل البريد الإلكتروني فقط، بلّ عليك التركيز على الطرق الأخرى التي تشمل الإتّصالات الهاتفية والرسائل النصيّة القصيرة ومواقع التواصل الاجتماعي أو الأخبار المزيّفة. يُمكنك الحصول على المواد الضرورية للتدريب على هذا الموضوع وزيادة المعرفة بشأنه من الملف الخاصّ بعنوان: مواد الدعم الخاصة بالهندسة الاجتماعية. إضافة لهذا، سنُقدّم لك رابطين إلى إثنين من الشرائط المرئية الخاصة ببرنامج الوعي الأمني من SANS، وهي متوافر أيضًا بلغات متعدّدة.

- الشريط المرئي بعنوان: الهندسة الاجتماعية (بالإنكليزية) متوافر أيضًا بلغات أخرى هنا
- الشريط المرئي بعنوان: التصيّد الاحتيالي (بالإنكليزية) متوافر أيضًا بلغات أخرى هنا

كلمات المرور المعقّدة

وفقًا لتقرير التحقيقات الخاصّة باختراق البيانات (DBIR) السنوي، فإنّ كلمات المرور السهلة ما تزال أهمّ أسباب اختراق البيانات عالميًا. هناك أربع سلوكيات أساسية تُساعد في إدارة هذا النوع من المخاطر وهي مذكورة أدناه. يُمكنك الحصول على المواد الضرورية للتدريب على هذا الموضوع وزيادة المعرفة بشأنه من الملف الخاصّ بعنوان: كلمات المرور.

- عبارات المرور (لاحظ أنّ فكرة كلمة المرور المعقّدة وفكرة صلاحية كلمة المرور قد أصبحتا من الماضي).
- استخدام كلمة مرور فريدة لكلّ من حساباتك
- برامج إدارة كلمات المرور
- نظام التحقّق من الهوية بعدّة عناصر (المعروف إختصارًا بـ MFA). الّذي يُعرف ايضًا بنظام التحقّق من الهوية بعاملين أو نظام التحقّق بخطوتين.

تحديثات الأنظمة

مواجهة نوع المخاطر الثالث تتمثّل بالتيقّن أنّ أيّ تقنية يستخدمها أفراد فرق العمل يجب أن تكون مزوّدة بآخر التحديثات الخاصّة بأنظمة التشغيل والبرامج وتطبيقات الأجهزة المحمولة. ويجب على الأشخاص الّذين يستخدمون أجهزتهم الشخصية تفعيل ميزة التحديث التلقائي. يُمكنك الحصول على المواد الضرورية للتدريب على هذا الموضوع وزيادة المعرفة بشأنه من الملفيّن الخاصّين بعنوان: برنامج ضارّ أو البيت الآمن إلكترونيًا.

مواضيع إضافية

- **واي–فاي:** تأمين نقطة الإتّصال اللاسلكية واي–فاي. تحدّثنا عن هذا الموضوع في مواد الملف البيت الآمن إلكترونيًا، يُمكنك أيضًا مشاهدة التسجيل المرئي بعنوان: البيت الآمن إلكترونيًا (باللغة الإنكليزية) متوافر أيضًا بلغات أخرى هنا.

- **الشبكة الخاصة الافتراضية (VPN):** ما هي الشبكة الخاصة الافتراضية (VPN) ولماذا عليك استخدامها. ننصحك بقراءة رسائل الإخبارية من OUCH عن موضوع الشبكة الخاصة الافتراضية (VPN).

- **العمل عن بُعد:** هذا موضوع مهمّ للّذين يعملون عن بعد ولكن خارج منازلهم، مثل العمل من المقهى أو المطار أو الفندق. ننصحك بمشاهدة التسجيل المرئي بعنوان: تدريب العمل عن بعد (باللغة الإنكليزية) متوافر أيضًا بلغات أخرى هنا.

- **الأولاد / الضيوف:** لزيادة الوعي بشأن عدم استخدام أفراد العائلة / الضيوف الأجهزة الخاصة بالعمل، ننصحك بمشاهدة التسجيل المرئي بعنوان: تدريب العمل عن بُعد (باللغة الإنكليزية) متوافر أيضًا بلغات أخرى هنا.

- **الرصد / الاستجابة:** هل تريد من الموظّفين الإبلاغ عن أيّ حادث أثناء العمل من المنزل؟ إذا كان جوابك نعم، فماذا تريد منهم الإبلاغ عنه ومتى؟ ستجد ما تبحث عنه في مواد ملف الاختراق .

رسائل OUCH الإخبارية

إضافة لكلّ ما ذكرناه سابقًا، نقترح عليك لدعم برنامجك تصفّح رسائل OUCH الإخبارية المترجمة لأكثر من 20 لغة. أضفنا لك أدناه مختارات من رسائل OUCH الاخبارية التي نرى أنّها تُمثّل أفضل مواد دعم لمبادرة العمل الآمن من المنزل. يُمكنك تصفّح كلّ الرسائل الإخبارية وترجماتها في أرشيف رسائل OUCH الإخبارية الخاصة بالوعي الأمني.

مواضيع أمنية عامّة

Four Steps to Staying Secure (أربع خطوات سهلة لتبقى بأمان)

https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (جعل المنزل آمن من الهجمات الإلكترونية)

https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

مواضيع الهندسة الاجتماعية

Social Engineering (الهندسة الاجتماعية)

https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (هجمات المراسلة)

https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (الحيل الشخصية)

https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (حيلة الرئيس التنفيذي / اختراق البريد الإلكتروني للعمل)

https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (الهجمات وعمليات الاحتيال عبر الهاتف)

https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (لا تكن فريسة سهلة)

https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (خداعك عبر وسائل التواصل الاجتماعي)

https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

مواضيع كلمات المرور

Making Passwords Simple (أنشئ كلمة مرور سهلة)

https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (تأمين بيانات الدخول)

https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

مواضيع إضافية

Yes, You Are a Target (نعم، أنت مستهدف)

https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (أجهزة المنزل الذكية)

https://www.sans.org/security-awareness-training/resources/smart-home-devices

نصائح سريعة

بعض النصائح والتوجيهات التي يُمكنك المشاركة فيها بسهولة.

- أكثر الخطوات فاعلية الّتي يُمكنك اتّخاذها لتأمين شبكتك اللاسلكية المنزلية هي تغيير كلمة مرور المشرف التي تأتي مع الجهاز من المصنع، ثمّ تفعيل نظام التشفير WPA2 واستخدام كلمة مرور معقّدة لشبكتك اللاسلكية المنزلية.
- حدّد واعرف كلّ الأجهزة المتّصلة بشبكتك المنزلية، بما في ذلك أجهزة مراقبة الأطفال وأنظمة الألعاب وأجهزة التلفاز والأجهزة المنزلية وحتى سيارتك. احرص على حماية كلّ هذه الأجهزة بكلمات مرور معقّدة وأنها تعمل بأحدث إصدارات أنظمة التشغيل.
- من أهمّ طرق حماية كمبيوترك في المنزل الحرص على أنّ نظام تشغيله وبرامجه مُحدّثة ومزوّدة بالتصحيحات الأمنية لضرورية. تذكّر تفعيل التحديث التلقائي عند الإمكان.
- في نهاية المطاف، يبقى التفكير السليم أفضل حماية لك. إذا بدا لك البريد الإلكتروني أو الاتّصال الهاتفي أو التراسل عبر الإنترنت غير مألوف

أو مريب أو غير واقعيّ، فقد يكون هذا هجومًا.

- احرص على استخدام كلمة مرور فريدة ومعقّدة لكلّ من حساباتك. ألا تستطيع تذكّر كلّ كلمات / عبارات مرورك؟ فكّر باستخدام برنامج إدارة كلمات المرور لحفظها كلّها بطريقة آمنة.
- نظام التحقّق بخطوتين يُعدّ واحدًا من أفضل الخطوات التي يُمكنك استخدامها لتأمين أيّ من حساباتك. ويطلب منك هذا النظام كلمة مرورك ورمز يُرسل إلى هاتفك المحمول أو رمز يُنتجه لك تطبيق خاص في جهازك. من الخدمات التي توفّر لك نظام التحقّق بخطوتين Gmail وDropbox وTwitter.
- التصيّد الاحتيالي هو حين يُحاول المهاجم خداعك للنقر على رابط ضارّ أو فتح مرفق يحمل فيروسًا وصلك بواسطة البريد الإلكتروني .كُن حذرًا من أيّ بريد أو رسالة إلكترونيين يتصنّعان حالة طارئة أو صيغت بطريقة ركيكة أو موجّهة لك بتحيّة عامّة مثل "عملينا العزيز."

المقاييس

إنّ تحديد المقاييس السلوكية في هذه الحالة ليس سهلًا لأنّ قياس طريقة تصرّف الناس في منازلهم أمرٌ صعب. إضافة إلى هذا، بعض هذه السلوكيات ليست خاصّة بالعمل (مثل تأمين شبكات واي–فاي اللاسلكية). لكنك تستطيع قياس التفاعل. لقد عرفنا من خلال الخبرة أنّ المواضيع الشخصية أو المشاعرية مثل الوضع الحالي تكون ذات قدر عالي من التفاعل وينتج عنها اهتمام أكبر مقارنة مع غيرها من المواضيع. لهذا سبب، نرى أنّ هذه المقاييس ستكون ذات قيمة.

- **التفاعل:** ما عدد المرّات التي يطرح فيها الناس أسئلة، أوّ يُقدّموا أفكارًا أو يطلبوا مساعدة عبر أيّ من القنوات أو المنتديات الأمنية التي تُشرف عليها وتديرها؟
- **تدريبات المحاكاة:** نفّذ نوعًا من تدريبات محاكاة الهندسة الاجتماعية، مثل هجمات التصيّد الاحتيالية، أو الهجمات بواسطة رسائل قصيرة أو إتّصالات هاتفية.

للحصول على قائمة مفصّلة بالمقاييس، يُمكنك تنزيل ملف مقاييس الوعي الأمني التفاعلي من ملف التنزيل الرقمي MGT433.

الترخيص

مؤلّف ملف خطّة العمل الطارئة

لانس سبيتزر خبير أمني منذ أكثر من 20 عامًا في مجالات أبحاث التهديدات الأمنية والهندسة الأمنية والوعي الأمني والتدريب الأمني. ساهم لانس في تطوير مجال الخداع والاستخبارات الإلكترونية من خلال إختراعه منظومة Honeynets وتأسيس مشروع Honeynet الأمني. بصفته مدربًا في معهد SANS Institute، عمل لانس على تطوير دورات MGT433: الوعي الأمني و MGT521: الثقافة الأمنية التدريبية. إضافة إلى كلّ هذا، نشر لانس ثلاثة كتب متخصّصة بالأمن، واستضيف في أكثر من 25 بلدًا للحصول على استشاراته وساعد أكثر من 350 منظمة في بناء برامج خاصة بالوعي الأمني والثقافة الأمنية لإدارة المخاطر البشرية. يستمر لانس في الظهور على وسائط مرئية وله حضور متواصل على موقع تويتر من خلال حسابه (@lspitzner) ويعمل على عدّة مشاريع أمنية مجتمعية. قبل تخصّصه في مجال أمن المعلومات، كان لانس ضابط مدرّعات في قوة التدّخل السريع العسكرية وقد حصل على شهادة الماجستير من جامعة إيلينوي.

عن معهد SANS Institute

تأسّس معهد SANS Institute عام 1989 ليكون منظمة تعليمية بحثية تعاونية. يعدّ معهد SANS Institute الجهة الكبرى والموثوقة التي تُقدّم تدريبًا وشهادات في مجال الأمن الإلكتروني للمختّصين المحترفين في المؤسّسات الحكومية والتجارية المنتشرة في جميع أنحاء العالم. أمّا المدرّبين في SANS Institute المعروفين عالميًا فيعملون في تدريس أكثر من 60 دورة تدريبية ضمن أكثر من 200 حدث مباشر تدريبي في مجال الأمن الإلكتروني وبواسطة الإنترنت أيضًا. وتعمل مؤسّسة GIAC التابعة لمعهد SANS Institute على مصادقة مؤهلّات المشاركين بواسطة أكثر من 35 شهادة تقنية عملية في مجال الأمن الإلكتروني. يُقدّم معهد SANS للتقنية (SANS Technology Institute)، وهو كيان تابع مستقّل ومُعتمد إقليميًا، شهادة ماجستير في علوم الأمن الإلكتروني. يُقدّم معهد SANS Institute موارد مجّانية متنوّعة لمجتمع إنفوسيك الأمني وتشمل هذه الموارد مشاريع إجماعية وتقارير أبحاث ورسائل إخبارية تقنية؛ ويُشغّل المعهد أيضًا مركز إنترنت ستورم (Internet Storm Center) الذي يُعدّ نظام تحذير مُبكر من الأخطار على الإنترنت. يضمّ معهد SANS Institute العديد من المختّصين الأمنيين الّذي يُمثّلون منظمات عالمية كثيرة تشمل شركات ضخمة وجامعات تعمل معًا لدعم ومساعدة مجتمع أمن المعلومات كلّه. (https://www.sans.org)