HUMANITAIRES JOBS · الأكاديمية الإنسانية

الميني MBA في الأمن وإدارة المخاطر: حماية الفرق والحفاظ على الوصول

مادة الدرس · الأسبوع 9 : الأمن الرقمي وحماية المعلومات

برنامج مدته 3 أشهر بالضبط (12 أسبوعًا، 144 ساعة) لإدارة الأمن والمخاطر في منظمة إنسانية: واجب الرعاية، وتحليل السياق، وتقييم المخاطر، والخطط والإجراءات، والقبول والتفاوض على الوصول، والحوادث، وإدارة الأزمات والاختطاف، وصحة الموظفين ورفاههم، والأمن الرقمي وحماية البيانات، ومخاطر المنظمة والامتثال، وتقاسم المخاطر مع الشركاء، والحوكمة واستمرارية الأعمال. تمارين رقمية مصححة، وثلاثة امتحانات شهرية مع دراسات حالة، ودبلوم قابل للتحقق من الأكاديمية الإنسانية.

https://humanitairejobs.org/ar/academy/mini-mba-securite-/risques/semaine-9

وثيقة مجانية من الأكاديمية الإنسانية. يمكن طباعتها ومشاركتها بحرية لأغراض التدريب دون تعديل.

الأسبوع 9 : الأمن الرقمي وحماية المعلومات

الأهداف

- تحديد التهديدات الرقمية الخاصة بالمنظمات الإنسانية: التصيّد الاحتيالي، الاحتيال في التحويلات، المراقبة، تسرّب البيانات.
- وضع تدابير أساسية متناسبة: المصادقة، النسخ الاحتياطي، التشفير، إدارة صلاحيات الوصول، الأجهزة.
- حماية بيانات الأشخاص الذين تجري مساعدتهم وبيانات الموظفين، والاستجابة لحادث رقمي.

لماذا يُعدّ المجال الرقمي خطرًا أمنيًا

تحتفظ المنظمات الإنسانية بمعلومات بالغة الحساسية: قوائم المستفيدين (أحيانًا مع بيانات بيومترية ومواقع)، شهادات عن الانتهاكات، بيانات طبية، معلومات عن الموظفين، تحليلات أمنية، تحركات. وقد يعرّض التسرّب أو الاختراق **أرواحًا** للخطر، لا البيانات فحسب.

استهدفت عدة هجمات سيبرانية معروفة منظمات إنسانية، بما في ذلك سرقة بيانات مئات الآلاف من الأشخاص المستضعفين. كما تُستهدف المنظمات بالاحتيال المالي عبر الإنترنت و**مراقبة** الاتصالات من قبل جهات حكومية أو من غير الدول.

التهديدات الرئيسية:

- **التصيّد الاحتيالي** (phishing): رسائل بريد إلكتروني أو رسائل مزيفة تسرق بيانات الدخول أو تثبّت برمجيات خبيثة.
- **الاحتيال في التحويلات**: مورّد مزيف، مدير مزيف يطلب دفعة عاجلة، تغيير احتيالي للبيانات المصرفية.
- **برمجيات الفدية**: تشفير البيانات مقابل فدية.
- **سرقة الأجهزة أو مصادرتها** (الحواسيب، الهواتف) عند نقاط التفتيش أو أثناء عمليات السطو المسلح.
- **مراقبة** الاتصالات وشبكات التواصل الاجتماعي.
- **الأخطاء الداخلية**: مشاركة عن طريق الخطأ، ملف أُرسل إلى المستلم الخطأ، كلمة مرور معروضة.

التدابير الأساسية

تمنع بعض التدابير البسيطة الغالبية العظمى من الهجمات الشائعة:

- **المصادقة متعددة العوامل** (MFA) على البريد الإلكتروني، والتخزين عبر الإنترنت، والمصرف، والبرنامج المحاسبي.
- **مدير كلمات المرور** وكلمات مرور طويلة وفريدة.
- **تحديثات** تلقائية للأنظمة والتطبيقات.
- **نسخ احتياطي** منتظم، منه نسخة غير متصلة بالشبكة أو معزولة، واختبارات للاستعادة (قاعدة 3-2-1: ثلاث نسخ، على وسيطين مختلفين، نسخة واحدة خارج الموقع).
- **تشفير** أقراص الحواسيب المحمولة والهواتف.
- **إدارة صلاحيات الوصول**: لا يصل كل شخص إلا إلى ما يحتاج إليه؛ وسحب صلاحيات الوصول يوم مغادرة الموظف.
- **تدريب** منتظم، مع تمارين محاكاة للتصيّد الاحتيالي.

مثال على تمرين. أرسل بريد تصيّد احتيالي مزيف إلى 120 موظفًا: نقر 38 على الرابط (31,7 %)، وأدخل 14 بيانات دخولهم (11,7 %)، وأبلغ 9 عن البريد إلى قسم المعلوماتية (7,5 %). وبعد تدريب موجَّه، أسفر تمرين ثانٍ عن 12 نقرة (10 %)، و3 عمليات إدخال (2,5 %)، و41 بلاغًا (34,2 %). ارتفاع البلاغات لا يقل أهمية عن انخفاض النقرات: فهو يحوّل الموظفين إلى نظام إنذار.

الاحتيال في التحويلات والإجراءات المالية

يكلّف **احتيال انتحال صفة المدير** والاحتيال المتعلق بالبيانات المصرفية المنظماتِ، بما فيها الإنسانية، مبالغ كبيرة كل عام. والإجراءات المالية هي أفضل وسيلة دفاع:

- يجري التحقق من أي **تعديل للبيانات المصرفية** لمورّد أو موظف بالاتصال على رقم معروف مسبقًا، وليس أبدًا على الرقم الوارد في الطلب.
- لا دفعة عاجلة خارج الإجراءات، حتى لو بدا أنها بطلب من مدير: يبقى الاعتماد المزدوج إلزاميًا.
- يجري الوصول إلى الخدمات المصرفية عبر الإنترنت بأجهزة وحسابات مخصصة، مع توقيع إلكتروني مزدوج.
- يعرف الموظفون أنهم سيحظون **بالدعم** إذا رفضوا دفعة مشبوهة، حتى لو طلبها رئيس أعلى.

> الاستعجال والسرية هما أداتا الضغط المفضلتان لدى المحتالين: «أنا في اجتماع، نفّذ هذا التحويل فورًا ولا تخبر أحدًا».

الأجهزة ونقاط التفتيش والمراقبة

في الميدان، المخاطر الرقمية **مادية** أيضًا:

- عند نقاط التفتيش، قد تُفتَّش الهواتف. والهاتف الذي يحتوي على صور لمواقع عسكرية، أو رسائل تنتقد أحد الأطراف، أو قوائم مستفيدين، قد يؤدي إلى الاحتجاز. القاعدة: عدم حمل سوى الضروري، حذف البيانات الحساسة من الأجهزة الميدانية، استخدام أجهزة مخصصة للعمل.
- تكشف **شبكات التواصل الاجتماعي** الخاصة بالموظفين معلومات قابلة للاستغلال: الموقع في الوقت الحقيقي، الآراء السياسية، صور الزملاء، علامات الثراء. وتقلّل سياسةٌ لاستخدام شبكات التواصل الاجتماعي، مشروحةٌ وغير عقابية، من هذه المخاطر.
- تحمي **تطبيقات المراسلة** المشفّرة من طرف إلى طرف المحتوى، لكنها لا تحمي واقعة التواصل نفسها، ولا الهاتف ذاته إذا صودر وهو غير مقفل.
- قد يكون استخدام بعض الأدوات (الأقمار الصناعية، الشبكات الافتراضية الخاصة VPN، الطائرات المسيّرة) محظورًا أو مثيرًا للريبة: يجب التحقق من التشريعات ومن القبول.

حماية بيانات الأشخاص

تقوم **حماية بيانات** المستفيدين والموظفين على مبادئ معترف بها (ولا سيما دليل اللجنة الدولية للصليب الأحمر وBrussels Privacy Hub بشأن حماية البيانات في العمل الإنساني):

- **المشروعية والغرض**: أساس مشروع وغرض محدد لكل عملية جمع.
- **تقليل البيانات إلى الحد الأدنى**: عدم جمع سوى ما هو ضروري.
- **الموافقة المستنيرة** عندما تكون هي الأساس المعتمد، مع مراعاة علاقات القوة (فالأسرة التي تحتاج إلى المساعدة ليست حرة في الرفض).
- **الأمن**: التشفير، تقييد صلاحيات الوصول، تسجيل العمليات.
- **الاحتفاظ المحدود** والحذف عند انتهاء الغرض.

- **المشاركة المؤطّرة** باتفاقات لتبادل البيانات، مع تحليل للمخاطر (بما في ذلك طلبات السلطات أو أطراف النزاع).
- **تقييم الأثر** قبل أي نظام جديد (البيانات البيومترية، الدفع عبر الهاتف المحمول، منصة مشتركة).

مثال على تقليل البيانات. لتوزيع حقائب، يجب تحديد هوية الأسرة والتحقق من أنها لم تتلقَّ الحقيبة من قبل. والانتماء العرقي أو الديني ليس ضروريًا ويجب ألّا يُجمع؛ وكذلك الصورة وبصمة الإصبع ليستا ضروريتين في العادة.

الاستجابة لحادث رقمي

يُعالَج الحادث الرقمي (حساب مخترَق، حاسوب مسروق، برمجية فدية، ملف أُرسل عن طريق الخطأ) كحادث أمني:

- **الاحتواء**: تغيير كلمات المرور، إلغاء الجلسات، عزل الجهاز المصاب، محو الجهاز المسروق عن بُعد.
- **التقييم**: ما البيانات، وما الأشخاص، وما الخطر عليهم؟
- **الإبلاغ**: الإدارة، مسؤول حماية البيانات، الأشخاص المعنيون إذا كانوا معرّضين لخطر، سلطات الرقابة وفق القانون الواجب التطبيق، المانحون وفق العقود.
- **الاستعادة** من النسخ الاحتياطية؛ وعدم دفع فدية دون قرار من الإدارة وتحليل قانوني.
- **التعلّم**: التحليل، التصحيحات، التدريب.

مثال. سُرق أثناء عملية سطو مسلح حاسوب محمول غير مشفّر يحتوي على قائمة 3 200 أسرة مع أرقام هواتفها ومواقعها. يتوقف الخطر على الأشخاص على السياق: فإذا كانت بعض الأسر تنتمي إلى مجموعة مستهدفة، يكون الخطر مرتفعًا. الإجراءات: تقييم فوري، إبلاغ المجتمعات المعنية عبر قنوات آمنة إذا كانت معرّضة للخطر، تغيير طرائق التواصل، تشفير إلزامي لجميع الحواسيب المحمولة.

تمرين: بريد إلكتروني عاجل من المدير

الوضع. يوم جمعة في الساعة 17:00، تتلقى المحاسبة بريدًا إلكترونيًا يبدو أنه من المدير القُطري، الموجود في مهمة خارج المكتب: «سري. يجب أن ندفع اليوم الدفعة المقدمة البالغة 48 000 دولار أمريكي لمورّد الوقود الجديد، وإلا خسرنا العقد. البيانات المصرفية مرفقة. لا يمكن الاتصال بي، اجتماع مع الوزير». يختلف عنوان المرسل بحرف واحد عن العنوان المعتاد. وفي اليوم نفسه، طلب مورّد معتاد عبر البريد الإلكتروني تغيير بياناته المصرفية. لا يتوفر في البريد الإلكتروني للمنظمة نظام مصادقة ثنائية.

المطلوب. 1) إشارات الإنذار. 2) التصرف الفوري. 3) التدابير الدائمة.

التصحيح. 1) الاستعجال، السرية، تعذّر الاتصال بصاحب الطلب، مورّد جديد دون ملف شراء، عنوان مرسل مختلف قليلًا، طلب موازٍ لتغيير البيانات المصرفية. 2) عدم الدفع؛ الاتصال بالمدير على رقمه المعروف (أو بنائبه)؛ عدم تعديل بيانات المورّد المعتاد دون اتصال تحقق على رقم معروف مسبقًا؛ الإبلاغ إلى مسؤول المعلوماتية وإلى الشؤون المالية؛ الاحتفاظ بالرسائل كأدلة. 3) مصادقة ثنائية على البريد الإلكتروني بأكمله؛ قاعدة مكتوبة: لا دفعة خارج الإجراءات، اعتماد مزدوج، تحقق هاتفي من أي تعديل مصرفي؛ تدريب وتمارين على التصيّد الاحتيالي؛ تصفية النطاقات المشابهة؛ رسالة واضحة من الإدارة: رفض أي دفعة مشبوهة سيحظى بالدعم دائمًا.

للتذكر

- البيانات الإنسانية حساسة: قد يعرّض التسرّب أرواحًا للخطر.
- المصادقة متعددة العوامل، كلمات مرور فريدة، التحديثات، النسخ الاحتياطي 3-2-1، التشفير، أدنى صلاحيات وصول، التدريب.
- الاحتيال في التحويلات: التحقق عبر رقم معروف، الاعتماد المزدوج، دعم من يرفض.
- الميدان: أجهزة مخففة المحتوى عند نقاط التفتيش، سياسة لاستخدام شبكات التواصل الاجتماعي.
- حماية البيانات: الغرض، التقليل إلى الحد الأدنى، الأمن، الاحتفاظ المحدود، تقييم الأثر.

الاختبار

1. تلقّى 150 موظفًا بريدًا مزيفًا؛ نقر 24 منهم. معدل النقر:
   A. 24 %
   B. 16 %
   C. 6,25 %
   D. 15 %

2. تعني قاعدة النسخ الاحتياطي 3-2-1:
   A. 3 نسخ، على وسيطين مختلفين، نسخة واحدة خارج الموقع
   B. 3 كلمات مرور، عاملان، حساب واحد
   C. 3 أيام، أسبوعان، شهر واحد
   D. 3 خوادم، بلدان، سحابة واحدة

3. يطلب مورّد عبر البريد الإلكتروني تغيير بياناته المصرفية. أنتم:
   A. تغيّرونها فورًا
   B. تدفعون نقدًا
   C. تردّون على البريد الإلكتروني
   D. تتحققون باتصال على الرقم المعروف مسبقًا

4. لتوزيع حقائب، جمع الانتماء العرقي للأسر:
   A. إلزامي
   B. موصى به
   C. مخالف لمبدأ التقليل إلى الحد الأدنى إذا لم يكن ضروريًا
   D. لا خطر فيه

5. سُرق حاسوب غير مشفّر يحتوي على قوائم مستفيدين. الخطوة الأولى:
   A. شراء حاسوب جديد
   B. تقييم البيانات المكشوفة والخطر على الأشخاص، ثم الإبلاغ
   C. عدم قول شيء
   D. نشر بيان صحفي

أجوبة الاختبار : 1. B · 2. A · 3. D · 4. C · 5. B