خطة الدرس

الحصة 3.1.2 (التكنولوجيا)

|  |  |  |  |
| --- | --- | --- | --- |
| الحصة 3.1.2 (التكنولوجيا والجريمة الإلكترونية) | | | **المدة: 150 دقيقة** |
| **الموارد المطلوبة:**   * كمبيوتر شخصي / كمبيوتر محمول مزود بنسخ برمجيات متوافقة مع المعدات المجهزة * جهاز العرض وشاشة العرض. * توصيلة الإنترنت (إن وجدت). * دفاتر وأقلام للطلاب. | | | |
| **الهدف من الحصة:**  ترمي هذه الحصة إلى تحديث معلومات المشاركين بشأن أنواع الجرائم والتهديدات الجديدة التي تطرحها التكنولوجيا الحديثة. وعلى الرغم من أن بعض المواضيع قد سبق التطرق إليها بإيجاز في الدورة التمهيدية، فإنها مطروحة مجددا بشكل أكثر تفصيلا في هذه الحصة. | | | |
| **الأهداف:**  في نهاية هذه الحصة، سيكون المشاركون قادرين على:   * شرح الأنواع المختلفة لاحتيال البريد الإلكتروني الخاص بالأعمال (BEC) * تحديد التهديدات التي يطرحها إنترنت الأشياء (IOT) * التمييز بين مختلف طبقات الإنترنت * شرح طريقة إنجاز المعاملات بالعملات الافتراضية. | | | |
| **توجيه المدرب**  تقدم هذه الحصة أحدث التكنولوجيات التي تؤثر على السلوك الإجرامي. وصدر تقرير "تقييم تهديدات الجريمة المنظمة على الإنترنت" (IOCTA) لعام 2017 في شهر سبتمبر من نفس السنة وتم استخدامه في بعض الشفافات باعتباره أحدث المعلومات المتاحة. وينبغي للمدربين مراجعة هذه المعلومات بعد صدور تقارير ومعلومات جديدة. وتعتبر الفيديوهات المستخدمة في هذه الحصة مقبولة ومتاحة للتحميل المجاني والاستخدام. وقد يرغب المدرب في الاستعانة بأمثلة للإيضاح كمنهاج تعليمي، مثلا في الحصة الخاصة بالشبكة المظلمة، عبر استخدام متصفح "تور" كي يوضح للمشاركين كيفية النفاذ إلى أدوات إجرامية على الإنترنت. | | | |
| محتوى الدرس | | | |
| رقم الشفافة | | المحتوى | |
| 1 إلى 3 | | تحدد الشفافات الأولى بنية وأهداف هذه الحصة. وسيمنح المشاركون فرصة لطرح أي أسئلة أولية قد تكون لديهم بشأن بنية وأهداف هذه الحصة. | |
| 4 إلى 18 | توفر هذه الشفافات معلومات حول تأثير الإنترنت على نطاق عالمي (الشفافات من 5 إلى 12) وتحديدا في البلد الذي تجري فيه الدورة التدريبية (الشفافات من 13 إلى 18). وينبغي أن يتأكد المدرب أن هذه الشفافات ذات الصلة بالبلد حيث تنفذ الدورة التدريبية وأن يستخدمها لمناقشة تأثير الإنترنت في البلد وفي السياق العالمي. | | |
| 19 إلى 30 | تعرض هذه الشفافات معلومات حول الجرائم الحديثة التي تحدث تأثيرا على مستوى هام. ينبغي أن يكون المدربون على علم بهذه الجرائم وأن يقدموا تلك التي تعتبر ذات صلة بمنطقة تقديم الدورة التدريبية. قد يرغب المدرب في استبدال بعض الحالات المستقاة من البلد. | | |
| 31 إلى 32 | تقدم هاتان الشفافتان معلومات مستخلصة من تقرير "تقييم تهديدات الجريمة المنظمة على الإنترنت" (IOCTA) لعام 2017 فيما يتعلق باحتيال البريد الإلكتروني الخاص بالأعمال (BEC). | | |
| 33 | يجب على المدرب أن يطرح على المشاركين السؤال المعروض على الشفافة. في حال عدم الحصول على إجابة، يمكنه مواصلة العرض. إذا كانت هنالك بعض الأمثلة، يجب عليه أن يخصص بعض الوقت للشروحات التي يقدمها المشاركون وأن يستخدم المعلومات المقدمة لمقارنتها مع المعلومات الواردة في العرض. | | |
| 34 إلى 42 | هذه الشفافات والفيديوهات مستخرجة من تريند مايكرو (Trend Micro)/ معلومات وبيانات يوروبول، وتوفر شرحا جيدا للغاية لمنهجيات احتيال البريد الإلكتروني الخاص بالأعمال والتدابير الوقائية. ويعرف الفيديو الأخير بالاحتيال بمحاكاة عمليات تجارية (Business Process Compromise/BPC) كنوع من أنواع احتيال البريد الإلكتروني الخاص بالأعمال. | | |
| 43 إلى 44 | تقدم هذه الشفافات موضوع إنترنت الأشياء (IOT). ينبغي للمدرب أن يدعو المشاركين إلى تقاسم أي معرفة أو تجربة لديهم بخصوص إنترنت الأشياء.  يرجى الانتباه إلى أن الشفافة رقم 45 عبارة عن فيديو يقدم مثالا جيدا للغاية عن كيف يمكن لمحرك عربة أن يكون متصلا بخدمات متعددة عبر إنترنت الأشياء وكيف يمكن لزبون أن يستفيد من هذه الخدمات بشكل كبير. ويمكن للمدرب أيضا التفكير في الأدلة الإلكترونية المتوفرة بفضل هذه الوصلات. | | |
| 45 | يقدم هذا الفيديو مثالا جيدا للغاية عن كيف يمكن لمحرك عربة أن يكون متصلا بخدمات متعددة عبر إنترنت الأشياء وكيف يمكن لزبون أن يستفيد من هذه الخدمات بشكل كبير. ويمكن للمدرب أيضا التفكير في الأدلة الإلكترونية المتوفرة بفضل هذه الوصلات. | | |
| 46 | توفر هذه الشفافة فرصة لتقديم النسخة السادسة لبروتوكول الإنترنت كمنصة تمكِّن إنترنت الأشياء. | | |
| 47 | توفر هذه الشفافة للمدرب فرصة لمناقشة قضايا أمن أجهزة إنترنت الأشياء ولتسليط الضوء على أن منتجي هذه الأجهزة ليسوا خبراء في مجال الأمن. وبالتالي، تعتبر أجهزة إنترنت الأشياء بمثابة قنبلة موقوتة من الناحية الأمنية. قد يرغب المدرب في المواصلة بالتطرق إلى النقاط البارزة بحسب معرفة المشاركين بالموضوع. | | |
| 48 إلى 49 | تقدم هاتان الشفافتان المزيد من المعلومات المحينة المستخلصة من تقرير "تقييم تهديدات الجريمة المنظمة على الإنترنت" (IOCTA) لعام 2017. وتدعم هذه المعلومات القضايا المطروحة في الشفافة 20. | | |
| 50 إلى 57 | توفر هذه الشفافات معلومات عن أجهزة إنترنت الأشياء وبعض القضايا ذات الصلة. ونحث المدربين على استخدام أمثلة يعرفونها، خاصة إذا ما كانت تنطوي على قضايا أمنية، على غرار القضية المرتبطة بغلاية الماء الإلكترونية (iKettle). | | |
| 58 إلى 60 | هذه الشفافات مدخل إلى الحصة حول الشبكة المظلمة والخدمات التي تعرضها. وتقدم هذه الشفافات السياق المستخلص من تقرير "تقييم تهديدات الجريمة المنظمة على الإنترنت" للشروع في مناقشة الموضوع. | | |
| 61 إلى 67 | تفسر هذه الشفافات الشبكة المظلمة، والاستخدام الإجرامي والخدمات الإجرامية بالإضافة إلى عرض بعض قصص النجاح في إعلاق مواقع كانت تستخدم لأنشطة إجرامية. ونشجع المدربين على تقديم توضيحات حية عن النفاذ إلى الشبكة المظلمة حيثما كان ذلك مناسبا وبتوفر وصلة إنترنت ملائمة. | | |
| 68 إلى 77 | تعتبر هذه الشفافات في الغالب تذكيرا بالقضايا المطروحة في الدورة التمهيدية مع دعمها بفيديوهات إضافية. وعلى غرار باقي المواضيع، استخلصت أحدث المعلومات من تقرير "تقييم تهديدات الجريمة المنظمة على الإنترنت" لعام 2017. | | |
| 78 إلى 79 | ينبغي للمدرب تلخيص أهداف الحصة مع المشاركين والتذكير بها ومنح المشاركين فرصة لطرح أي أسئلة ذات الصلة بالمواد التي تطرقت إليها هذه الحصة. | | |
| **تمارين تطبيقية**  لا توجد أي تمارين تطبيقية إلزامية، ومع ذلك نشجع المدربين على تقديم توضيحات حية عن النفاذ إلى الشبكة المظلمة حيثما كان ذلك مناسبا. | | | |
| **التقييم/التحقق من المعرفة**  لم يتم إعداد أي تقييم رسمي لهذه الدورة التدريبية. ويتوقع من الحضور المشاركة بنشاط وحيوية. | | | |