الكتيب 7.1: تقييم الأمن السيبراني

الغرض: تقديم الأسئلة التي تساعد على مناقشة الأمن السيبراني مع مدراء تكنولوجيا المعلومات

ستساعد الأسئلة التالية المشاركين لمناقشة الأمن السيبراني مع مدراء تكنولوجيا المعلومات في الوكالات التي يعملون بها بغرض تقييم مستوى الأمن الإلكتروني الخاص بأنظمة المعلومات في البنية الأساسية الحرجة - هل تقوم وكالتك أو منظمتك بالإجراءات التالية:

- **استخدام أسلوب أمني يحد من البرامج التي يمكن تشغيلها في وقت واحد؟**
  - **تطبيق نظام القائمة البيضاء**: أسلوب أمني استباقي حيث يتم السماح فقط لعدد محدود من البرامج الموثوقة بالعمل دون سائر البرامج (بما في ذلك البرمجيات الضارة) حيث يتم منعها من العمل من الأساس؛ ويتم التحكم عن طريق الإدارة وليس المستخدمين لتحديد البرامج التي سيتم السماح لها بالعمل
  - يختلف هذا الأسلوب عن معظم أنظمة التشغيل المعيارية الموحدة التي تسمح لجميع المستخدمين بتحميل وتشغيل أي برنامج يختارونه - بما في ذلك البرامج التي تحتوي على برمجيات ضارة مخبأة بها والتي قد تكون حديثة ولا يمكن كشفها بالبرمجيات المضادة للفيروسات
  - لا يجب استخدام هذا الأسلوب منفرداً ولكن كجزء من استراتيجية دفاعية عميقة تنطوي على برامج مكافحة الفيروسات والجدران النارية
- **ضمان أن جميع تحميلات البرامج وتحديثاتها آتية من مصادر مضمونة؟**
  - عادة ما يستهدف عناصر التسلل المضادة أجهزة الكمبيوتر غير المحدثة - فهم على علم بالثغرات والضعفات التي تعتري البرامج القديمة وكيفية استغلالها لاختراق الكمبيوتر
  - وأفضل ممارسات قسم تكنولوجيا المعلومات هو وضع برنامج إدارة يقوم بمراقبة جميع التحديثات المرخصة من برامج موثوقة مع التحقق من مصادرها - ويتم منع كافة التحديثات البرمجية من سائر المواقع غير المعروفة أو المشبوهة
  - لا يجب السماح لمستخدمي أجهزة الكمبيوتر والحاسوب المحمول بتحميل برامج وتحديثات بدون تصريح من قسم تكنولوجيا المعلومات
- **عزل الشبكات من أية مواقع غير موثوقة خصوصاً المواقع الشبكية الإلكترونية؟**
  - إذا كان هناك متطلبات محددة للعمل بالوصول إلى شبكات خارجية فيتعين تقليص زمن التواصل مع تلك الشبكات
  - يتعين مراقبة الوظائف التي تتم خلال وقت التواصل بالشبكات الخارجية
- **هل يتم فصل نظام الكمبيوتر في أجزاء منفصلة ومتميزة؟**
  - يتم احتواء كل قسم وهكذا يصبح من الأسهل احتواء الأزمة عند اختراق أحد الأقسام بحيث لا يتم اختراق باقي الأجزاء تلقائياً
  - يجب تقييد المرور بين أقسام الاتصال الإلكتروني
  - يمكن استمرار الاتصال العادي ولكن يجب إيقاف أي دخول غير مرخص
  - يمكن الحد بسهولة من التدمير المحتمل الناتج عن التسلل
  - ويمكن تنظيف الأجهزة بعد حادث التسلل بتكلفة أقل لقسم واحد تعرض للإصابة بدلا من تنظيف النظام بجملته

- **هل تتوافر سياسة صارمة لإصدار وترخيص الاطلاع على الوثائق داخل النظام؟**
  - بدأت عناصر التسلل المعادية بالتركيز على السيطرة على الحصول على مؤهلات شرعية للدخول، خصوصاً عند التعامل مع الحسابات عالية التميز حتى يمكنهم التباهي بأنهم من المستخدمين المشروعين
  - إذا ظن النظام أن مستخدم شرعي يقوم بدخول النظام، فلن تنطلق أية إنذارات تنبيه عن عملية تسلل ولن يكون هناك أي دليل على عملية تسلل
  - يجب تقليص مميزات المستخدم بحيث يتم الدخول فقط للبرامج المطلوبة بحسب الحاجة وفقاً للواجبات المناطة لهذا المستخدم
  - يجب تطبيق استخدام سياسات كلمة المرور أو الكودات السرية لتأكيد الطول على التعقيد، وفرض مؤهلات فريدة لكل برنامج، وفرض تغيير كلمات المرور السرية كل 90 يوم على الأقل
  - الاحتفاظ بكافة معلومات التأهيل في أنظمة منفصلة عن تلك المستخدمة
- **هل يتم السيطرة على الدخول عن بعد والتأكد من المؤهلات ومحدوديات الوقت؟**
  - إذا تم السماح بدخول النظام بعيداً عن موقع البنية الأساسية الحرجة، فيتعين مراجعة الاستخدام والمستخدمين مع وضع تقييدات صارمة على الدخول - ويتضمن ذلك أجهزة المودم الملحقة بالفاكس والتي تعتبر غير آمنة إلى حد كبير
  - استخدام نمطين من المؤهلات إن أمكن مثل كلمات المرور المعقدة مع كلمات سر قوية وأسئلة أمنية صعبة
  - وضع قيود على عدد عمليات النفاذ المتبقية ووقت النفاذ لباقي المستخدمين - مع استبعاد أي مستخدمين فوراً بمجرد تخطي العدد المسموح بالدخول والوقت المصرح به - والتحول إلى نظام نمط الدخول الذي يسمح بالنفاذ فقط (وهو أكثر أمناً من نظام القراءة فقط).
- **هل يتم مراقبة النظام باستمرار والاستجابة الفورية لحوادث التسلل؟**
  - يتطلب الدفاع عن أجهزة الكمبيوتر الخاصة بأنظمة البنية الأساسية الحرجة المراقبة النشطة ضد عمليات التسلل المعادية وسرعة تنفيذ الاستجابة المعدة لذلك
  - يتعين أن تتم المراقبة في المناطق التي يتم بها عمليات اتصال غير عادي أو مشبوه، أو التي تحتوي على تحميلات ضارة، أو محاولات اختراق، أو تحليل مفاتيح الدخول (الوقت والمكان، مثلا، لسرقة مؤهلات الاستخدام والدخول غير المأذون من موقع غريب، ثم التحقق عن طريق مكالمة هاتفية بالمستخدم المصرح له)، ومحاولات المستخدم لتغيير مواصفات السيطرة الأمنية
  - ضمان توافر خطط الاستجابة في حالة تأهب حتى تتحقق الاستجابة الفورية إذا تم كشف عملية تسلل - تتضمن أمثلة على الاستجابات فصل جميع وصلات الإنترنت، وإيقاف حسابات المستخدمين، عزل الأنظمة المشبوهة بالإضافة إلى البحث عن البرامج المتسللة، وتطبيق نظام تغيير كامل 100 بالمائة لكلمات السر في شتى أنحاء الوكالة