الدليل الإجرائي للتعامل مع الاختراقات وتفاديها في الجمعية

الدليل الإجرائي للتعامل مع الاختراقات وتفاديها

الصادرعن: إدارة التقنية والأمن السيبراني - الجمعية

ص.ب 51384 الرياض 11543- المملكة العربية السعودية – هاتف 96614198833 + – فاكس 966114190033 + ترخيص رقم 2063
P.O.BOX 51384 RIYADH 11543- KINGDOOM OF SOUDI ARBIA – TEL : +96614198833 - FAX: +966114190033 - LICENSE NO.2063
www.Modeem.org.sa

الهدف:

تحديد خطوات الاستجابة والتعامل مع أي اختراق أمني أو هجمات سيبرانية محتملة على أنظمة الجمعية، وبيان الإجراءات الوقائية لتفاديها مستقبلاً.

أولاً: تعريف الاختراقات

الاختراق هو أي وصول غير مصرح به إلى أنظمة المعلومات أو البيانات أو الأجهزة الخاصة بالجمعية ويشمل:

- سرقة أو تسريب بيانات.
- تعطيل الأنظمة.
- الدخول إلى البريد الإلكتروني أو الحسابات الاجتماعية بطريقة غير شرعية.
- تثبيت برمجيات ضارة أو فيروسات.

من الضروري اتخاذ إجراءات وقاية كاملة من حيث يقدر القراصنة على الوصول إلى الأجهزة الإلكترونية بمهارة فائقة وبطرق غير متوقعة على الإطلاق، وما تحتاج إلى فهمه هو كيف ينعكس ذلك على ما يظهر لك على الشاشة.

نقدم لك فيما يلي بعض المؤشرات المحتملة التي توضح أنك تعرضت للاختراق، بالإضافة إلى بعض الاقتراحات لحلول سريعة وعملية.

1. **ملاحظة أي شيء غير طبيعي يحدث على شاشة الكمبيوتر** .في الأغلب أنت تستخدم الكمبيوتر يوميًا، وبالتالي من الطبيعي أن تعرفه وتعرف طريقة عمله أكثر من أي شخص آخر. إذا كنت تعمل على الجهاز بشكل طبيعي لكن فجأة أصبح نظام التشغيل يقوم بأفعال غريبة، فالأسباب وراء ذلك قد ترجع إلى قدم مكونات الكمبيوتر أو وجود تلف من نوع أو آخر، لكن العلامات التالية تحديدًا قد تشير كذلك إلى تعرض الجهاز إلى الاختراق:

- يوجد لديك برامج أو ملفات أساسية لا تعمل بشكل طبيعي أو ترفض أن يتم فتحها من الأساس
- اختفاء بعض الملفات على الرغم من أنك لم تحذفها، إذ تجدها محذوفة تمامًا أو تم نقلها إلى سلة المهملات.
- لا تقدر على تشغيل البرامج باستخدام كلمة السر المعتادة.ربما تجد أن كلمات السر الخاصة بك تم تغييرها.
- يوجد برنامج أو أكثر تم تثبيته على الكمبيوتر دون أن تكون أنت الطرف الذي قام بهذا الأمر.
- يوصل الكمبيوتر نفسه بشبكة الإنترنت بشكل متكرر في أوقات عدم استخدامك له.

ص.ب 51384 الرياض 11543- المملكة العربية السعودية – هاتف 96614198833 + – فاكس 966114190033 + ترخيص رقم 2063
P.O.BOX 51384 RIYADH 11543- KINGDOOM OF SOUDI ARBIA – TEL : +96614198833 - FAX: +966114190033 - LICENSE NO.2063
www.Modeem.org.sa

- تم تغيير محتوى بعض الملفات دون أن تكون أنت الطرف الذي قام بهذه التغييرات.
- تصدر الطابعة خطوات غريبة. ربما ترفض طباعة ما توجهه لها من أوامر طباعة أو أن تطبع صفحات مختلفة عما حددته لها.

2. **اتصل بالإنترنت** .يمكنك من خلال هذه الخطوة أن ترى الكثير من العلامات الدالة على تعرضك للاختراق.

- يرفض موقع أو أكثر أن يتم عملية تسجيل دخولك إليه بسبب تغيير كلمة السر. جرب مجموعة من المواقع التي تزورها بشكل معتاد؛ إذا لم تنجح كلمة السر الخاصة بك، فقد يرجع السبب وراء ذلك إلى تعرضك للاختراق. هل قمت بالتفاعل مع أي من رسائل البريد الإلكترونية المؤذية عن طريق الخطأ (أو رسالة بريد إلكتروني محتالة تطلب منك تحديث كلمة السر أو تغيير خيارات الأمان)؟
- يتم إعادة توجيه نتائج البحث الخاصة بك.
- تظهر نوافذ إضافية من متصفح الإنترنت. يمكن أن يتم تشغيل وإغلاق هذه النوافذ دون أن تفعل أي شيء؛ ربما تكون هذه النوافذ ذات لون أكثر قتامة إلا أنك سوف تكون قادرًا على رؤيتهم.
- إذا قمت بشراء اسم نطاق إلكتروني، فربما أنك غير قادر على الوصول إليه بمجرد إتمامك لعملية الشراء.

3. **ابحث عن المزيد من البرامج الضارة التي يُضيفها المخترقون إلى أجهزة الكمبيوتر** .فيما يلي بعض الاحتمالات الإضافية لما يمكن أن تراه على جهازك في حالة تعرضك للاختراق:

- تستقبل رسائل مزيفة تخبرك بوجود فيروسات على الكمبيوتر. إما أنك تمتلك برمجية للحماية من الفيروسات على الكمبيوتر أو لا؛ في الحالة الأخيرة سوف تظهر لك هذه الرسائل لإخبارك كذبًا عن وجود فيروسات قادرة على إتلاف محتويات الجهاز، أما في الحالة الأولى فالمفترض أنك تعرف شكل رسائل البرنامج المضاد للفيروسات، لذلك انتبه في حالة كان شكل الرسائل مختلفًا عما تعتاد عليه. لا تضغط على أي رابط أو تتفاعل مع هذه الرسائل والتي تحاول الاحتيال عليك بهدف تشجيعك على إدخال بياناتك الشخصية أو المالية الخاصة ببطاقة الائتمان وغير ذلك بعد إيهامك أن ذلك سوف يساعدك على التخلص من الفيروسات على الجهاز. انتبه إلى أن المخترق يتحكم بالفعل في الكمبيوتر (اطلع على الأجزاء التالية لمعرفة ما يجب عليك فعله).
- تظهر شرائط أدوات إضافية في متصفح الإنترنت، وربما تحمل رسائل تدعي مساعدتك! يجب أن يوجد شريط أدوات واحد فقط أو الشرائط التي قمت بتثبيتها بنفسك. اشعر بالشك في حالة ظهر لك أي قوائم أو شرائط إضافية.
- تظهر لك نوافذ منبثقة عشوائية ومتكررة على الكمبيوتر. تحتاج إلى معرفة البرنامج الذي يتسبب في هذا الأمر والتخلص منه.

ص.ب 51384 الرياض 11543- المملكة العربية السعودية – هاتف 96614198833 + – فاكس 966114190033 + ترخيص رقم 2063
P.O.BOX 51384 RIYADH 11543- KINGDOOM OF SOUDI ARBIA – TEL : +96614198833 - FAX: +966114190033 - LICENSE NO.2063
www.Modeem.org.sa

- لا يعمل برنامج مكافحة الفيروسات والبرامج الضارة ويبدو أنه غير متصل. قد يتم إيقاف إمكانية استخدام "مدير المهام" أو "محرر سجل النظام."
- يصل إلى الأفراد الموجودين في قائمتك البريدية رسائل مزيفة وتحمل روابط ضارة.
- تفقد أموال من حسابك البنكي أو تصلك فواتير دفع لمشتريات إلكترونية لم تشرها من الأساس.

4. **إذا كنت ببساطة لا تملك أي تحكم فيما يحدث على الكمبيوتر، توقع بنسبة كبيرة أنك ضحية لعملية اختراق** . قد تجد في بعض الحالات أن مؤشر الفأرة يتحرك على الشاشة من تلقاء نفسه وينفذ أوامر لم توجهها له على الإطلاق، ويكون ذلك إشارة مؤكدة على وجود طرف بشري في مكان ما في العالم قد نجح في الوصول إلى داخل الكمبيوتر ويتلاعب بك. ربما أنك تعرف ما نقصد الحديث حوله في حالة استخدامك لأي من برامج التحكم في أجهزة الكمبيوتر عن بعد أو كنت قد سمحت لأحد العاملين في صيانة الكمبيوتر أن يعمل على إصلاح جهازك عن بعد كذلك. أي حركة تظهر أمامك دون أن تكون أنت المسؤول عنها، فهذه إشارة لا جدال حولها على تعرضك للاختراق.

- افحص معلوماتك الشخصية. ابحث عن نفسك عبر موقع البحث جوجل. هل تجد أي نتائج شخصية لم تنشرها بنفسك من قبل؟ قد لا تظهر هذه النتائج في الحال، لكن إبقاء عينك منتبهة إلى هذا الاحتمال قد يكون بالغ الأهمية لكي تسارع بحماية خصوصيتك في حالة ظهور أي من معلوماتك الشخصية عبر الإنترنت.

ثانياً: الإجراءات الفورية عند حدوث اختراق

1. **التبليغ الفوري :**

-على أي موظف يلاحظ اختراقاً أو سلوكًا مشبوهًا، إبلاغ المسؤول التقني فورًا أو عبر البريد الرسمي للأمن السيبراني.

2. **عزل النظام :**

-فصل الجهاز أو الشبكة المصابة من الإنترنت فورًا لمنع امتداد الضرر.

3. **فتح تحقيق تقني :**

-يبدأ القسم التقني بتحليل الهجوم لتحديد نوع الاختراق، مصدره، وبياناته المتأثرة.

4. **النسخ الاحتياطي :**

-التأكد من سلامة النسخ الاحتياطية وحفظها في أماكن غير متصلة بالشبكة.

ص.ب 51384 الرياض 11543- المملكة العربية السعودية – هاتف 96614198833 + – فاكس 966114190033 + ترخيص رقم 2063
P.O.BOX 51384 RIYADH 11543- KINGDOOM OF SOUDI ARBIA – TEL : +96614198833 - FAX: +966114190033 - LICENSE NO.2063
www.Modeem.org.sa

5. **تغيير كلمات المرور :**

-تغيير جميع كلمات المرور للأنظمة المتأثرة.

-يتضمن وصف الحادث، توقيته، الأنظمة المصابة، الضرر الناتج، والإجراءات التصحيحية.

ثالثاً: الإجراءات الوقائية لتفادي الاختراقات

1. **التدريب والتوعية :**

إجراء ورش عمل دورية لجميع الموظفين عن الأمن السيبراني.

2. **سياسة كلمات المرور :**

-إلزام جميع الموظفين باستخدام كلمات مرور قوية، وتحديثها كل 90 يومًا.

3. **النسخ الاحتياطي المنتظم :**

-تنفيذ نسخ احتياطي تلقائي أسبوعي للأنظمة والملفات المهمة.

4. **التحديثات الأمنية :**

-تحديث جميع البرامج والأنظمة بشكل منتظم.

5. **استخدام برامج الحماية :**

-تثبيت جدار حماية (Firewall) وبرمجيات مضادة للفيروسات.

6. **سياسة الوصول :**

-تحديد صلاحيات الدخول لكل مستخدم وفقًا لدوره في الجمعية

ص.ب 51384 الرياض 11543- المملكة العربية السعودية – هاتف 96614198833 + – فاكس 966114190033 + ترخيص رقم 2063
P.O.BOX 51384 RIYADH 11543- KINGDOOM OF SOUDI ARBIA – TEL : +96614198833 - FAX: +966114190033 - LICENSE NO.2063
www.Modeem.org.sa

رابعاً: جهات التنسيق

- القسم التقني: تحليل الحادث، تنفيذ الحماية، التبليغ الداخلي
- إدارة الجمعية: اتخاذ قرارات عليا، التواصل الخارجي (إن لزم)
- الموارد البشرية : متابعة التوعية والتدريب
- الإدارة القانونية : التعامل مع الآثارالقانونية (إن وجدت)

خامساً: التوثيق والمتابعة

يجب أرشفة جميع تقارير الحوادث السيبرانية في ملف خاص ضمن إدارة التقنية، وتقديم تقرير فصلي لمجلس الإدارة عن أي أحداث أو محاولات اختراق.

ص.ب 51384 الرياض 11543- المملكة العربية السعودية – هاتف 96614198833 + – فاكس 966114190033 + ترخيص رقم 2063
P.O.BOX 51384 RIYADH 11543- KINGDOOM OF SOUDI ARBIA – TEL : +96614198833 - FAX: +966114190033 - LICENSE NO.2063
www.Modeem.org.sa