/https://medium.com

الأمن السيبراني لمواقع الشبكات الاجتماعية . التحديات والحلول

Priya Reddy

ترجمة وتنقيح – المهندس احمد الربيعي

الغرض الرئيسي من مواقع الشبكات الاجتماعية هو تحقيق الارتباط بين المستخدمين والمنظمات فقد طورت العديد من الفرص التجارية للشركات ، كما أدخلت وسائل التواصل الاجتماعي تغييرات مهمة في طريقة التواصل اذ تبرز مواقع الشبكات الاجتماعية اهتمام محدد يتعلق بخصوصية المستخدم وأمنه. كما يركز أمان وخصوصية هذه المواقع بشكل أساسي على اكتشاف البرامج الضارة ، حيث يبدو أنها تأتي من جهة اتصال موثوق بها لذلك من الأرجح أن يقوم المستخدمون بالنقر على الرابط. شكلت مواقع الشبكات الاجتماعية تطبيقات في العديد من المجالات مثل :

- **التجارة الإلكترونية الاجتماعية :** يمكن استخدام مواقع الشبكات الاجتماعية لإعلانات اصحاب بوابة التجارة الإلكترونية.
- **العلامة التجارية :** توفر وسائل التواصل الاجتماعي منصة أفضل للشركات بغية جذب العملاء لمزيد من فرص العمل .

القضايا

نظرًا لأن نمو مواقع الشبكات الاجتماعية قد حقق العديد من الفوائد ، فقد جلب أيضًا العديد من المخاوف الأمنية. كما انه يوفر منصة عرضة للاستغلال من قبل المهاجمين. بعض القضايا المرتبطة هي على النحو التالي :

١. **إساءة استخدام الهوية :** يقوم المهاجم بانتحال هوية أي مستخدم . وينتج عنه إساءة استخدام تلك الهوية حيث يقوم بذلك من خلال التطبيقات التي يطلب فيها منح إذن للوصول إلى المعلومات المقدمة في مواقع الشبكات الاجتماعية. فعندما يسمح أحد المستخدمين بالقيام بذلك ، سيحصل المهاجم على حق الوصول إلى جميع المعلومات ويمكن إساءة استخدام هذه المعلومات دون علم المستخدم.

٢. **تهديدات من استخدام تطبيقات الجهات الخارجية :** تسعى هذه التطبيقات للحصول على إذن من المستخدم للوصول إلى المعلومات الشخصية لجميع الألعاب والتطبيقات المختلفة. اذ يقوم المستخدم بمنح التطبيق مستوى معينًا من الإذن فيما يتعلق بمعلوماته . وقد تقوم بعض هذه التطبيقات بتنزيل برامج ضارة على كمبيوتر المستخدم أو هاتفه دون موافقته.

٣. **الوثوق بمشغلي مواقع الشبكات الاجتماعية :** المحتويات التي يقوم المستخدم بتحميلها أو نشرها على مواقع الشبكات الاجتماعية ، تكون متاحة مع مشغلي الشبكات. حيث يمكن للمشغلين حفظ بيانات الحساب حتى بعد الحذف.

٤. **الفيروسات وهجمات التصيد والبرامج الضارة :** غالبًا ما تجد الفيروسات والبرامج الضارة طريقها إلى جهاز الكمبيوتر الخاص بك من خلال تلك الإعلانات المزعجة. بعد الوصول إلى الشبكة ، يمكن للمهاجم سرقة البيانات السرية عن طريق نشر رسائل البريد العشوائي .

٥. **المشكلات القانونية :** نشر محتويات مسيئة لأي فرد أو مجتمع أو بلد. هناك مخاطر قانونية مرتبطة باستخدام مواقع الشبكات الاجتماعية مثل تسريب المعلومات السرية على المواقع أو اقتحام خصوصية شخص ما.

٦. **تتبع المستخدمين :** يمكن أن يتسبب ذلك في مخاوف أمنية مادية للمستخدم ، حيث يجوز للأطراف الثالثة الوصول إلى معلومات التجوال للمستخدم من خلال جمع التحديث في الوقت الحقيقي على موقع المستخدم.

٧. **خصوصية البيانات :** يقوم المستخدمون بمشاركة معلوماتهم على مواقع الشبكات الاجتماعية ويمكن أن يتسببوا في وجود قيود خصوصية ما لم يتم تطبيق تدابير أمنية مناسبة. على سبيل المثال ، يمكن للجميع الاطلاع على معلومات المستخدم إذا كان الإعداد الافتراضي للمستخدم هو (عام - public) حيث يمكن أن يؤدي قبول الطلبات من أشخاص مجهولين أيضًا إلى إنشاء تهديد أمني.

المخاطر والتحديات

مع زيادة عدد المستخدمين على مواقع الشبكات الاجتماعية ، فقد اتاح هذا طرقاً جديدة للمهاجمين للوصول إلى حسابات الأفراد. المزيد من المعلومات المنشورة يخلق تهديدا جديدا على خصوصية وأمن المستخدم . المواقع الاجتماعية تنمو بسرعة وتشكل مخاطر جديدة للأفراد والمؤسسات في هذا العالم الحديث للتكنولوجيا. وبعض التحديات هي كما يلي :

١. **هجمات التصيد :** إنها تقنية هجومية تهدف الى الوصول للمعلومات الحساسة. اذ يقوم المهاجمون بإنشاء صفحات ويب مزيفة تشبه الصفحات الشرعية ويطلبون من المستخدمين إدخال بيانات اعتمادهم ويواجه المستخدم مشكلة عندما يدخل المستخدم إلى بيانات الاعتماد. فقد كشفت إحصائيات Kaspersky Lab أن المواقع الاجتماعية المزيفة التي تحاكي حسابات مستخدمي Facebook تشكل ما يقارب 22% من هجمات التصيد الاحتيالي في عام 2014. ووفقًا لهذه الاحصائية فإن التصيد الاحتيالي يمثل تهديدًا كبيرًا في روسيا وأوروبا مع زيادة عدد الهجمات في هذه المنطقة ، بزيادة 18% لتصل إلى 36.3 مليون هجوم في الربع الثالث من عام 2015 مقارنة بنفس الفترة من العام الماضي. على سبيل المثال ، قام رجل من مولدوفا بإدارة خطة تصيد احتيالي انتهت بخسارة قدرها 3.5 مليون دولار لشركة حفر في غرب بنسلفانيا .

٢. **تحديات مطابقة الهوية :** هي تقنية تستخدم لمشاركة بيانات اعتماد المستخدم عبر مجالات متعددة. على سبيل المثال ، تقدم العديد من المواقع للمستخدمين إمكانية تسجيل الدخول بحسابهم على Facebook بحيث يكون أكثر ملاءمة للمستخدم ، وليس عليه إنشاء حسابات متعددة عبر مواقع مختلفة. قد يبدو هذا مناسبًا ولكن المستخدم ليس لديه معلومات حول كيفية وإلى أي مدى يمكن مشاركة معلوماته الشخصية بين تطبيقات الطرف الثالث.

٣. **البرامج الضارة :** هي البرامج المثبتة في أجهزة المستخدم دون علم المستخدم وموافقته. وهي تنتشر بسرعة وتصيب الأجهزة وتشمل : فيروسات البرمجيات ، وأحصنة طروادة . حيث يمكن للمهاجمين الوصول إلى المعلومات الشخصية للمستخدم من خلال مراقبة أنشطة الكمبيوتر ويمكن أيضًا التحكم في جهاز الكمبيوتر أو القيام بهجمات جماعية دون علم المستخدم حيث يمكن للبرامج الضارة سرقة هوية المستخدم وتعطيل الاجهزة . أيضًا ، يمكن للمتطفلين تثبيت أشكال من البرامج الدعائية التي يمكن أن تتسبب في ظهور إعلانات منبثقة لا حصر لها على جهاز المستخدم مثل :

- **فيروس LOL :** ينتشر هذا الفيروس من خلال وظيفة الدردشة على Facebook. حيث يتم إرسال هذا الفيروس إلى المستخدم بصفة رابط مرفق به وعندما يقوم المستخدم بالنقر عليه ، يتم تنزيل البرامج الضارة إلى نظام المستخدم. وتصيب النظام وتنتشر عبر الشبكة للوصول إلى معلومات المستخدم.
- **Zeus :** هذا هو حصان طروادة الذي ينتشر عن طريق النقر على الرابط ليقوم بمسح جميع الملفات الموجودة على نظام المستخدم وسرقة المعلومات المهمة. تخصص هذا الفيروس هو سرقة أوراق اعتماد البنك للمستخدم .

٤. **النقر فوق هجمات الاصطياد :** تسمى أيضًا هجمات تعويض واجهة المستخدم. حيث يطلب Trojan في صفحات الويب من المستخدم النقر فوق الارتباط الضار ، ويتم زرع برامج ضارة على النظام. يعد هذا أمرًا شائعًا في Facebook .

التوصيـــــــــات

في هذا القسم ، سيتم تقديم بعض التوصيات لتأمين معلومات المستخدم وهي :

- بالنسبة لشركة ما ، يجب وضع بعض السياسات الخاصة برسائل البريد الإلكتروني بحيث لا يتم الخلط بين هذه الرسائل وأي رسائل بريد إلكتروني غير مرغوب فيها أو رسائل تصيّد
- يجب أن يستخدم كل من المستخدم والمنظمة نوعية جيدة من برامج مكافحة الفيروسات حتى تتمكن من تصفية المواقع الضارة وحظرها
- يجب أن تتم المصادقة على كل مستوى من مواقع الويب لتجنب وصول المهاجمين إلى معلومات المستخدم الشخصية
- يجب استخدام التقنيات المعتمدة على التشفير لضمان أمان معلومات المستخدم المقدمة على مواقع الشبكات الاجتماعية. تبادل مفتاح المجموعة ، واستخراج البيانات ، والتشفير هي بعض الأمثلة التي يمكن استخدامها لتعزيز الأمن على وسائل التواصل الاجتماعي
- ينبغي أن تنفذ الحكومة برامج تدريبية وتثقيفية لنشر الوعي حول الأمن السيبراني. كما يتوجب إجراء حملات وبرامج دعائية تتضمن ندوات ومسابقات ومعارض حول الأمن السيبراني
- تتناول مواقع الشبكات الاجتماعية التي تحتوي على إعداد أمان الخصوصية الأدوات المتاحة لجعل الحساب أكثر أمانًا. مثل إعدادات الخصوصية في Facebook حيث تنقسم أساسيات الخصوصية إلى :

١. **من يستطيع رؤية (هذا) :** هذا هو إعداد الأولوية لمستخدمي Facebook حيث يمكن للمستخدم الحد من الجمهور الذي يمكنه رؤية المشاركات من المستخدم. يجب تجنب المشاركات العامة
٢. **تنبيهات تسجيل الدخول :** يتيح هذا الإعداد للمستخدم الحصول على إشعار عندما يقوم أي شخص بتسجيل الدخول إلى حسابه من جهاز أو مستعرض غير معروف.
٣. **المصادقة الثلاثية :** هذا هو الإعداد الجديد الذي تمت إضافته إلى Facebook والذي يتيح إنشاء رمز أمان Facebook لمصادقة أي تطبيق تابع لجهة خارجية
٤. **كيف يتفاعل الآخرون مع المستخدم :** يساعد هذا المستخدم على إدارة كيفية تأثير نشاط الآخرين على ملف تعريف المستخدم. كما يمكن للمستخدم إدارة العلامات أو (إلغاء التعارف) أو (حظر) شخص ما.

- **إعدادات أمان متصفح الويب :** وتشمل :

١. يجب على المستخدم تحديث المستعرضات وتمكين التحديثات التلقائية للمتصفح
٢. حظر المكونات الإضافية ، والنوافذ المنبثقة ، ومواقع الخداع.
٣. قم بضبط المتصفح على وضع (عدم تخزين كلمات المرور)
٤. تعطيل ملفات تعريف ارتباط الطرف الثالث
٥. إعدادات خاصة بالمتصفح :

- **Firefox :** قم بتثبيت الوظيفة الإضافية NoScript
- **Safari :** تعطيل Java
- **IE :** إعداد نطاقات الأمان

الخلاصـــــــــة

مع تزايد شعبية مواقع الشبكات الاجتماعية ، فقد أصبحت هدفاً رئيسياً للهجمات والجرائم الإلكترونية . وامتدت الجريمة السيبرانية على نطاق واسع لتشكل تهديدًا كبيرًا للأمن القومي والاقتصادي. ان المؤسسات العامة والخاصة في قطاعات الصحة العامة والمعلومات والاتصالات والدفاع والخدمات المصرفية والمالية في خطر. لذلك يجب على المنظمات اتخاذ تدابير أمنية مناسبة لتكون آمنه من الجرائم الإلكترونية ، كما يتوجب على المستخدمين حماية معلوماتهم الشخصية لتجنب سرقتها أو إساءة استخدامها.

أصبح الفضاء الإلكتروني مجالًا مهمًا للجرائم الإلكترونية والإرهابية للهجوم على المعلومات الهامة. لذلك ، هناك حاجة إلى تعاون عالمي من الأمم للعمل سوية بغية الحد من تهديد الإنترنت المتزايد باستمرار.