الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

حماية البريد الإلكتروني

رصد مركز أمن المعلومات في الهيئة الوطنية لخدمات الشبكة عدة هجمات إلكترونية استهدفت مخدمات البريد الإلكتروني التابعة لجهات عامة وخاصة لنشر برمجيات خبيثة على الشبكة السورية، وقد استغلت ضعف إجراءات الحماية المتبعة لتأمين هذه المخدمات أو مستخدميها.

ولذلك تم التعميم على كافة الجهات العامة بضرورة اتخاذ إجراءات الحماية المناسبة للتصدي لهذه الهجمات، ويوصي مركز أمن المعلومات لكافة الجهات العامة والخاصة بضرورة الحيطة والحذر، لاستدراك ما يمكن أن ينجم عن حالات اختراق البريد الإلكتروني من عواقب مثل تسرب البيانات أو الاستخدام السيئ لحسابات البريد الإلكتروني كأدوات لجرائم معلوماتية يعاقب عليها القانون.

ونقدم لكم فيما يلي بعض النصائح والإجراءات الواجب اتباعها لحماية خدمة البريد الإلكتروني:

1. فرض استخدام كلمات مرور قوية على كافة الحسابات المعرفة على مخدم البريد الإلكتروني، وتغيير كافة كلمات المرور للحسابات الحالية، وضرورة مراجعة وتدقيق جميع الحسابات المعرفة على مخدمات البريد الإلكترونية، ومطابقتها مع المستخدمين الفعليين لاكتشاف وجود حسابات مجهولة وإلغائها.
2. اعتماد آليات وأدوات لفحص وفلترة البريد الإلكتروني (ANTI-SPAM, ANTI-VIRUS) قبل تمريرها من وإلى المرسل أو المستقبل عبر مخدم البريد الإلكتروني، ويمكن ذلك من خلال تجهيزات أو برمجيات مخصصة لهذا الغرض، حيث تقدم تجهيزات Next Generation Firewalls الحماية اللازمة لمخدمات البريد الإلكتروني.
3. تحديث برنامج تشغيل المخدم المضيف بشكل دائم.
4. تنصيب برمجيات مضادة للبرمجيات الخبيثة على طرفيات المستخدمين تدعم حماية البريد الإلكتروني.

5. ضبط صلاحيات تشغيل الملفات التنفيذية على طرفيات العاملين بما يتناسب مع طبيعة عملهم، خصوصاً طرفيات العاملين الإداريين على مختلف مستوياتهم.
6. استخدام الشهادة الرقمية ssl لضمان تشفير حركة البيانات بواسطة بروتوكولات البريد الإلكتروني (imap.http,pop3,smtp)
7. توعية مستخدمي البريد الإلكتروني من كافة المستويات الإدارية والفنية بعدم فتح مرفقات البريد الإلكتروني المرسلة من حسابات مجهولة، وضرورة إعلام مسؤول أمن المعلومات أو مدير النظام عند وجود أي بريد مشبوه لاتخاذ الإجراءات المناسبة، وعدم استخدام حساباتهم البريدية للتسجيل في أي مواقع خارجية أو محلية خارج إطار متطلبات عملهم لأن ذلك قد يجعلها تتعرض لهجمات باستخدام رسائل البريد الواغل (SPAM).
8. اتخاذ الإجراءات اللازمة لإلغاء الحسابات البريدية للعاملين فور انتفاء الحاجة لها مثل حالات النقل- الاستقالة- التقاعد-الندب ... الخ.
9. توثيق ضوابط حماية البريد الإلكتروني ضمن سياسة أمنية خاصة ومتابعة تطبيقها والالتزام بها من قبل مسؤول أمن المعلومات.

إعداد

مركز أمن المعلومات

دمشق 2022/8/31