Process Safety Beacon
رسائل للعاملين في الصناعة
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

هذا العدد برعاية من
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

الأمن السيبراني والعمليات الكيميائية

يوليو 2021

هل تعلم؟

- يستخدم مجرمو الإنترنت برامج ضارة معقدة للاستفادة من نقاط الضعف المتعددة وتحقيق أهدافهم.
- تتزايد هجمات برامج الفدية مع استخدام المجرمين المنظمين لها كأداة لكسب المال.
- وفقًا لدراسة حديثة ، يحدث هجوم إلكتروني كل 39 ثانية. (راجع https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- التصيد الاحتيالي هو إرسال رسائل بريد إلكتروني ، يفترض أنها من شركات مرموقة ، لحث الأفراد على الكشف عن معلومات شخصية. هذه الهجمات هي طريقة إدخال أساسية للبرامج الضارة.
- يمكن أن تدخل التهديدات الإلكترونية إلى أنظمة الشركة من خلال رسائل البريد الإلكتروني والمرفقات ومن أجهزة التخزين المحمولة ، مثل محركات الأقراص المصغرة أو أجهزة التخزين المحمولة الأخرى.
- خمسة وتسعون بالمائة من انتهاكات الأمن السيبراني ناتجة عن خطأ بشري. (راجع https://www.cybintsolutions.com/employee-education-reduces-risk/)

ماذا تستطيع أن تفعل

- تحقق دائمًا من طلبات تحديث البرامج مع قسم تكنولوجيا المعلومات قبل المتابعة وتثبيت التحديثات المعتمدة في الوقت المناسب.
- تأكد من تحديث جدران الحماية وبرامج الشبكة الأخرى وتشغيلها.
- تأكد من عمل نسخة احتياطية لأنظمتك وبياناتك بانتظام.
- استخدم كلمات مرور قوية لجميع الوصول. لا تشارك كلمات المرور أو الحسابات وقم بتغيير كلمات المرور بانتظام.
- لا تحفظ كلمات المرور على المتصفحات.
- لا تنقر على الروابط أو المرفقات في رسائل البريد الإلكتروني المرسلة من شخص لا تعرفه.
- لا تقم أبدًا بتثبيت البرامج غير المعتمدة على أي كمبيوتر شركة ؛ تأكد من تأمين مفاتيح الوصول وأجهزة الأمان المادية الأخرى بشكل صحيح.
- إذا كنت تستخدم الوصول عن بُعد ، فاتبع متطلبات الشركة. كن يقظًا بشكل خاص عند استخدام مواقع الإنترنت العامة.
- إذا كان هناك شيء ما على جهاز الكمبيوتر الخاص بك يبدو غريبًا أو مختلفًا ، فاطلب المساعدة! قد يكون أحد المتسللين يحاول الوصول.

الشكل 1. أولدسمار ، محطة معالجة المياه في فلوريدا

في 5 فبراير 2021 ، لاحظ موظف في محطة معالجة المياه في أولدسمار بولاية فلوريدا أن المؤشر يتحرك بشكل غريب على شاشة كمبيوتر التحكم ، في البداية ، لم يكن هناك أي قلق ؛ استخدم المصنع برنامج الوصول عن بُعد للسماح للموظفين بمشاركة الشاشات واستكشاف مشكلات تكنولوجيا المعلومات وإصلاحها. غالبًا ما يتصل المشرف بجهاز كمبيوتر المشغل لمراقبة أنظمة المنشأة أيضًا. بعد بضع ساعات ، لاحظ المشغل تحرك المؤشر والنقر فوق عناصر التحكم في محطة معالجة المياه. في غضون ثوانٍ ، كان الدخيل يحاول تغيير نقطة ضبط هيدروكسيد الصوديوم في النظام من 100 جزء في المليون (جزء في المليون) إلى 11100 جزء في المليون. اكتشف المشغل التسلل بسرعة وأعاد هيدروكسيد الصوديوم إلى المستويات الطبيعية. لحسن الحظ ، لم يكن هناك أي تأثير على جودة المياه.

أدى هجوم فدية مؤخرًا على خط أنابيب كولونيال إلى إيقاف إمدادات البنزين إلى الساحل الشرقي للولايات المتحدة لعدة أيام.

من المحتمل أن تكون أنظمة شركتك متصلة بالإنترنت وتحتاج إلى الحماية من التهديدات الإلكترونية. هناك العديد من الاستراتيجيات التي تستخدمها الشركات لردع التهديدات السيبرانية مثل: جدران الحماية وبرامج مكافحة الفيروسات وسياسات الحماية من البرامج الضارة وفيروسات الكمبيوتر.

المزيد من الناس يعملون عن بعد ؛ زاد هذا من فرص الهجمات الإلكترونية.

الهجمات الإلكترونية حقيقية. أنت جزء حيوي من الدفاع.