Hackeado

Translation powered by

Distritos escolares en guardia contra ataques de ransomware

El año pasado se reportaron más de 100 ataques cibernéticos en distritos escolares.

Mire los distritos escolares desde la perspectiva de un hacker.

Los distritos mantienen una gran cantidad de información confidencial sobre empleados, estudiantes y familias, todo en línea y accesible en diversos grados a cientos o miles de empleados, no todos los cuales prestaron especial atención en el seminario web de seguridad cibernética obligatorio de este año. Con presupuestos anuales de decenas o cientos de millones, sus bolsillos son profundos, al menos en teoría, con el fin de pagar el rescate.

Y no pueden darse el lujo de no recuperar sus datos.

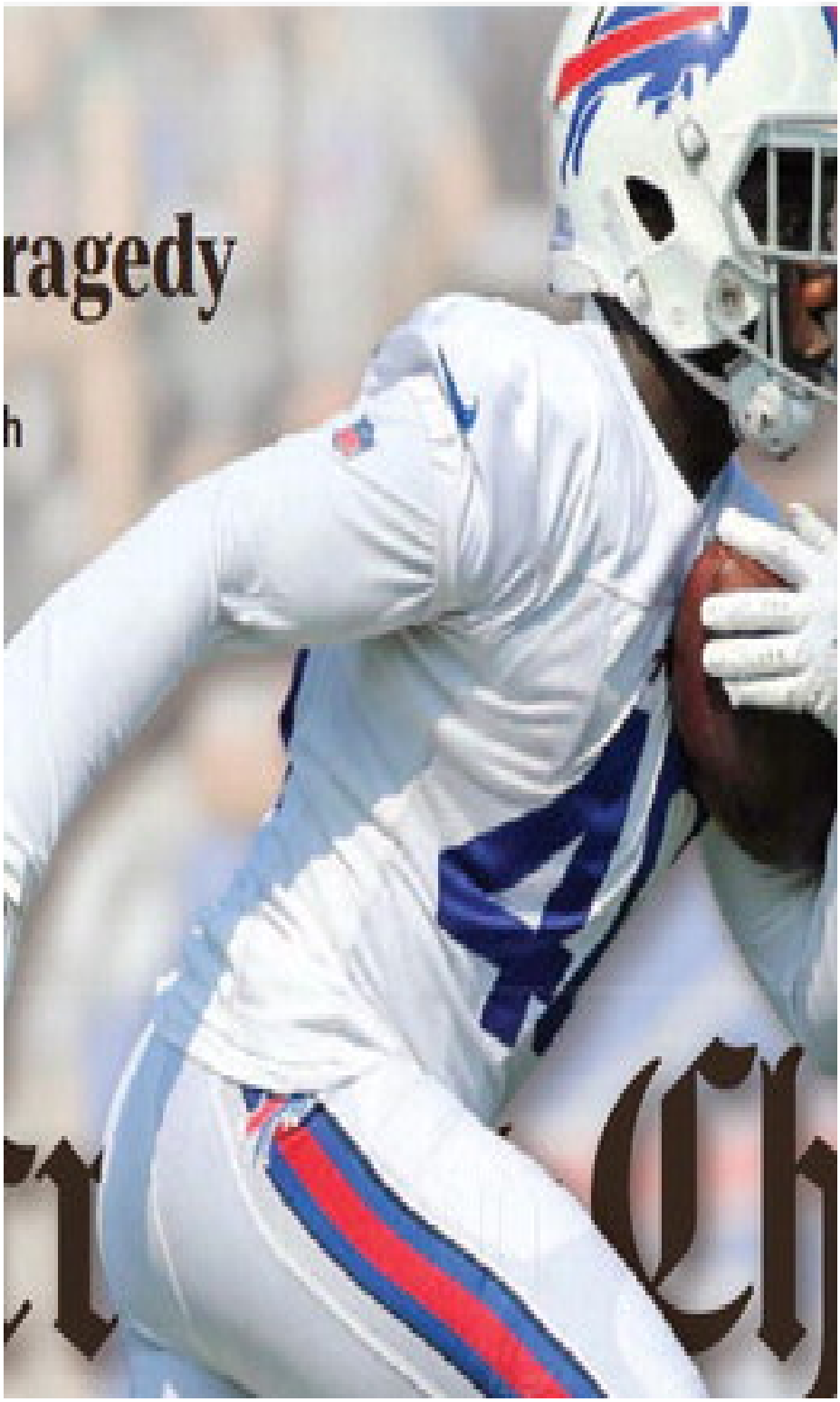
"En la lista de cosas que me mantienen despierto por la noche, es muy importante", dijo John Miller, director de tecnología, evaluación de datos y programas en el Distrito Escolar Hilton Central.

“Si le preguntas a cualquier persona relacionada con la tecnología en el campo, te dirán lo mismo. ... Ninguno de nosotros quiere que esto nos suceda ".

Más de 100 distritos escolares estadounidenses informaron ataques cibernéticos en 2018, probablemente un recuento significativo bajo de un evento inherentemente sensible. Al menos tres distritos escolares del área de Rochester han sido objeto de ataques en los últimos años.

Más recientemente, el Distrito Escolar de la Ciudad de Syracuse y la Biblioteca Pública del Condado de Onondaga fueron víctimas de un ataque de ransomware aparentemente originario de Europa del Este. El ransomware es un software que bloquea parte o la totalidad de un sitio web hasta que el propietario paga el rescate, generalmente en una moneda cibernética difícil de rastrear, como Bitcoin.

GETTY IMAGES Los **alumnos de kindergarten Inieris Santiago, delantero, Shuaib Hussein, trasero izquierdo, y Bryan Miller, trabajan en computadoras en 2018 durante una unidad de actividad rotativa en la escuela 8.** JAMIE GERMANO / ROCHESTER DEMÓCRATA Y FOTO DE ARCHIVO DE CRÓNICAS



"Creo que el ransomware está creciendo como un vector de ataque porque funciona y porque la gente paga", dijo Bill Stackpole, profesor de seguridad informática en el Instituto de Tecnología de Rochester. “El problema principal en este momento es que no hay realmente una buena defensa contra eso. Solo hace falta una persona para hacer clic en algo en lo que no deberían estar haciendo clic ".

Eso significa que un empleado cae en un intento de phishing, haciendo clic en un archivo adjunto de aspecto inocuo que desata un virus en la red a la que está conectada su computadora.

Para un distrito escolar, los objetivos potenciales de información incluyen los números de cuenta bancaria o los registros de personal de los empleados, así como la información médica, académica y disciplinaria de los estudiantes. Otros datos podrían tener que ver con proveedores, conexiones policiales o problemas legales delicados.

Algunas de esas cosas, por ejemplo, los números de Seguro Social de los empleados, son fáciles de vender en línea para los hackers de blackhat. Los registros académicos no tienen el mismo valor en efectivo, pero, dijo Stackpole, son "pivotables" para su uso en un ataque de ingeniería social.

Por ejemplo, dijo, un pirata informático que sabe que cierto estudiante está luchando en matemáticas podría hacerse pasar por su maestro en un correo electrónico de phishing. Cuando la estudiante hace clic en un archivo adjunto que cree que es una hoja de trabajo con práctica adicional en fracciones, su computadora también se infecta .

Distritos locales afectados

La piratería de Syracuse conmovió a los distritos de Nueva York, pero particularmente en el distrito escolar de la ciudad de Rochester, que se encuentra en una situación similar. Su directora de tecnología, Annmarie Lehner, dijo que las amenazas de seguridad cibernética han estado "aumentando exponencialmente" durante los últimos años, con intentos de phishing en la parte superior de la lista. Dos veces en los últimos años, dijo, los piratas informáticos que se hacen pasar por administradores de alto nivel han enviado correos electrónicos a los empleados de nómina que intentan cambiar su cuenta bancaria de depósito directo. Ningún intento funcionó, dijo, en parte debido a una mayor capacitación y niveles adicionales de seguridad.

De alguna manera, los distritos escolares pequeños son el objetivo más tentador, ya que probablemente tienen menos salvaguardas establecidas. El Distrito Escolar Central de Holley, por ejemplo, vio información personal sobre miles de empleados y contratistas expuestos en una violación en 2016. Dos distritos locales han sido infiltrados en el último año por sus propios estudiantes. En Honeoye Falls-Lima en octubre pasado, los estudiantes obtuvieron acceso a los registros académicos al piratear la cuenta del superintendente . En mayo, un niño de 17 años de la escuela secundaria Gates Chili fue arrestado por ocho cargos de delito grave después de ingresar a la cuenta suspendida del ex superintendente y acceder a imágenes de cámaras de seguridad, registros académicos e informes de asistencia, entre otras cosas. "Esto tiene el aspecto de una película de Hollywood", dijo el jefe de policía de Gates, Jim VanBrederode. "Es un estudiante de secundaria sentado con su tableta emitida por la escuela".

Representantes de Holley y Gates Chili declinaron hacer comentarios. Honeoye Falls-Lima no respondió a las solicitudes de comentarios, ni Grecia, el distrito escolar suburbano más grande del condado de Monroe, ni el Departamento de Educación del estado.

En caso de duda, haga clic en 'eliminar'

Hay dos formas principales para que un distrito escolar u otra organización juegue defensa contra el ransomware y otros ataques cibernéticos: barreras técnicas y capacitación.

Los primeros incluyen, en el extremo superior, software sofisticado para el cual las escuelas a menudo carecen de la experiencia y el presupuesto necesarios. Los medios más comunes incluyen la verificación en dos pasos para iniciar sesión en dispositivos de forma remota o marcar el correo electrónico que proviene de cuentas externas.

Lehner, de RCSD, asiste a una conferencia anual para oficiales de tecnología escolar y generalmente regresa con algún truco nuevo para mantener seguras las computadoras de los empleados.

"Todos los años vuelvo ... y todos dicen: 'Dios mío, Annmar, es decir, volverá'", dijo. "Porque saben que tendré algo nuevo que hacer".

"Sabemos como (oficiales de información en jefe) que necesitamos implementar estas características, pero hemos tenido un retroceso porque es un dolor en el trasero". Ahora que la gente ve que sucede en el mundo real, están un poco más de aceptación ".

Más valioso es inculcar en los empleados un escepticismo saludable en términos de lo que hacen clic.

"Presiono 'borrar' mucho", dijo Stackpole. "Mi enfoque de la vida en este momento es: si es necesario hacer clic en lo que me enviaste, puedes hacer que mi teléfono suene".

JMURPHY7 @ Gannett. com

Friday, 08/02/2019 Page .A01