Cómo hacer frente a la ciberseguridad en las aulas y más allá

La **ciberseguridad afecta a todas las industrias** y esto no es diferente cuando se trata del sector educativo. A medida que continuamos innovando y progresando en un mundo digital, las amenazas aumentan de forma exponencial, y la ciberdelincuencia es un desafío creciente para las instituciones educativas. Desde **escuelas, hasta colegios y universidades**, todos los departamentos educativos pueden estar en riesgo de un ciberataque.

Uno de los muchos desafíos es la **administración de la seguridad de los *endpoints***. A medida que los teléfonos inteligentes, tabletas y computadoras portátiles se dirigían a las aulas, el riesgo de una violación de datos aumentó. El mayor riesgo es el acceso remoto de profesores y estudiantes que se conectan a la red desde casa. La actual pandemia mundial ha catapultado este desafío con los administradores de TI que ahora deben gestionan un entorno de trabajo remoto complejo casi de la noche a la mañana.

Los campus y escuelas de todos los tamaños sufren ataques que pueden poner en peligro la información. La **privacidad de los estudiantes** sobre la inscripción, los apellidos, las direcciones de casa y otra información confidencial de identificación personal también se puede poner en peligro. Cualquier dato que proporciona información personal es una mina de oro para los delincuentes cibernéticos. Las escuelas y universidades a menudo también cuentan con datos sobre los parientes cercanos y otros detalles familiares, todo lo cual es invaluable. De hecho, una institución de educación superior informó recientemente de 118 ciberataques exitosos en un plazo de seis meses, lo que representa el 13% de todas las infracciones, lo que convierte a la educación superior en el tercer sector objetivo, solo detrás de la atención sanitaria y las finanzas.

Los ciberdelincuentes a menudo buscan una manera de **explotar las vulnerabilidades** de las instituciones para entrar en la red. El desafío es que con más dispositivos conectados hay un número creciente de puntos de acceso (posibles vulnerabilidades). La proliferación de dispositivos con acceso a la red e información de las instituciones ha aumentado el riesgo de un ataque, dado que casi todos los empleados y estudiantes han tenido que trabajar de forma remota durante la pandemia. Todos estos dispositivos y puntos de acceso necesitan administrarse. Si las instituciones permiten el **Bring Your Own Device**, por sus siglas en inglés, desde conexiones Wi-Fi hasta contraseñas de usuario y, en algunos casos, la aplicación de parches está ahora fuera del control inmediato de TI. Y cada dispositivo que utiliza la red es un posible vector de ataque.

Antes del golpe de la pandemia, los organismos educativos estaban empezando a examinar la mejor manera de implementar políticas de BYOD y algunos departamentos tenían procesos avanzados. Pero incluso los equipos de TI más preparados han tenido restos importantes para manejar el aumento significativo que ha traído la pandemia. La mayor adopción de dispositivos remotos significa que fundamentalmente los equipos de TI ahora tienen menos visibilidad en los dispositivos conectados a la red, hay más puntos de acceso débiles potenciales para los delincuentes cibernéticos y, por lo tanto; posiblemente menos control y seguridad. Los delincuentes cibernéticos también buscan atacar desde lugares desconocidos por el área de IT.

Este es un desafío a largo plazo, principalmente cuando comenzamos a ver la transición de vuelta al aula, lo que nos hace ver que todavía habrá un repunte significativo en el número de dispositivos remotos.

Realizar un seguimiento de estos nuevos dispositivos, plataformas, aplicaciones y tecnologías puede parecer abrumador, especialmente a la luz de la pandemia. Entonces, ¿cómo pueden los departamentos de TI superar algo que se siente como una tarea imposible?

Muchos equipos de TI pasan demasiado tiempo preocupándose por **los riesgos de brechas de seguridad**. Los administradores de TI necesitan tener el ancho de banda y la capacidad de ser proactivos, mantenerse al día con la última tecnología y participar en la planificación de la tecnología y la toma de decisiones para mitigar los riesgos cibernéticos. Realmente deben garantizar que los equipos tengan visibilidad completa y utilizar herramientas de administración de dispositivos móviles, modernas o tradicionales.

Una vez que los departamentos de TI han obtenido la visibilidad tan necesaria en los dispositivos remotos, es más fácil controlar posibles puntos débiles. La **ciberdelincuencia** no va a desaparecer, por lo que es importante salvaguardar y reducir los riesgos potenciales. Esto se puede hacer a través de la gestión de inventario, asegurando que cada dispositivo remoto tenga software de seguridad implementado y automatizando la administración de parches y el análisis de vulnerabilidades. Ya sea que los dispositivos remotos sean de propiedad corporativa o personales, cada uno de ellos es un punto de acceso contra el que los departamentos de TI deben protegerse. Quest cuenta con herramientas que le permiten a las áreas de IT la administración automatizada de esos dispositivos y brindan el máximo nivel de seguridad.

Si los equipos de TI pueden rastrear fácilmente el inventario, administrar y proteger fácilmente los dispositivos móviles que acceden a sus redes de campus/escuela, entonces estarán en una mejor posición para reforzar la **seguridad cibernética**. Mediante el uso de la automatización, los administradores de TI también pueden proporcionar la capacidad de guardar la configuración preconfigurada en los dispositivos, para facilitar la implementación de las políticas de seguridad. Esto evitará que los departamentos de TI se inunden con solicitudes de configuración sencillas.

Fundamentalmente cualquier punto final desde cámaras, memorias USB o teléfonos portátiles, puede plantear un desafío de seguridad. No podemos evitar el aumento de los dispositivos remotos que llegan al aula y se conectan a la red de las instituciones, pero los equipos de TI pueden empezar a proteger la red asegurándose de que tengan visibilidad de cada dispositivo que se conecta.

En resumen, la automatización es fundamental para permitir que los equipos de TI puedan hacer frente al desafío cada vez más creciente importante de la administración de *endpoints y la implementación de las políticas de seguridad.* Aquellas áreas de TI que pueden monitorear y tener información sobre dispositivos remotos en toda su red estarán en una posición justa para protegerse contra las amenazas a la seguridad cibernética.