Guía para la ciberseguridad durante la pandemia de COVID-19

mexus®
Managed secure IT | no matter what

Guía para la ciberseguridad durante la pandemia de COVID-19

Según los resultados de la encuesta de impacto de la pandemia de las OSC, el 61% de los encuestados de seguridad y líderes de TI están preocupados por un aumento en los ataques cibernéticos dirigidos a sus empleados que trabajan desde casa. Según la encuesta, 26% ha visto un aumento en el volumen, la gravedad y / o el alcance de los ataques cibernéticos desde mediados de marzo.

Esta guía de recursos proporciona información sobre ciberataques comunes que actualmente se informan. También proporciona recursos para mejorar la higiene cibernética para mejorar las defensas cibernéticas, tanto para las organizaciones como para sus empleados.

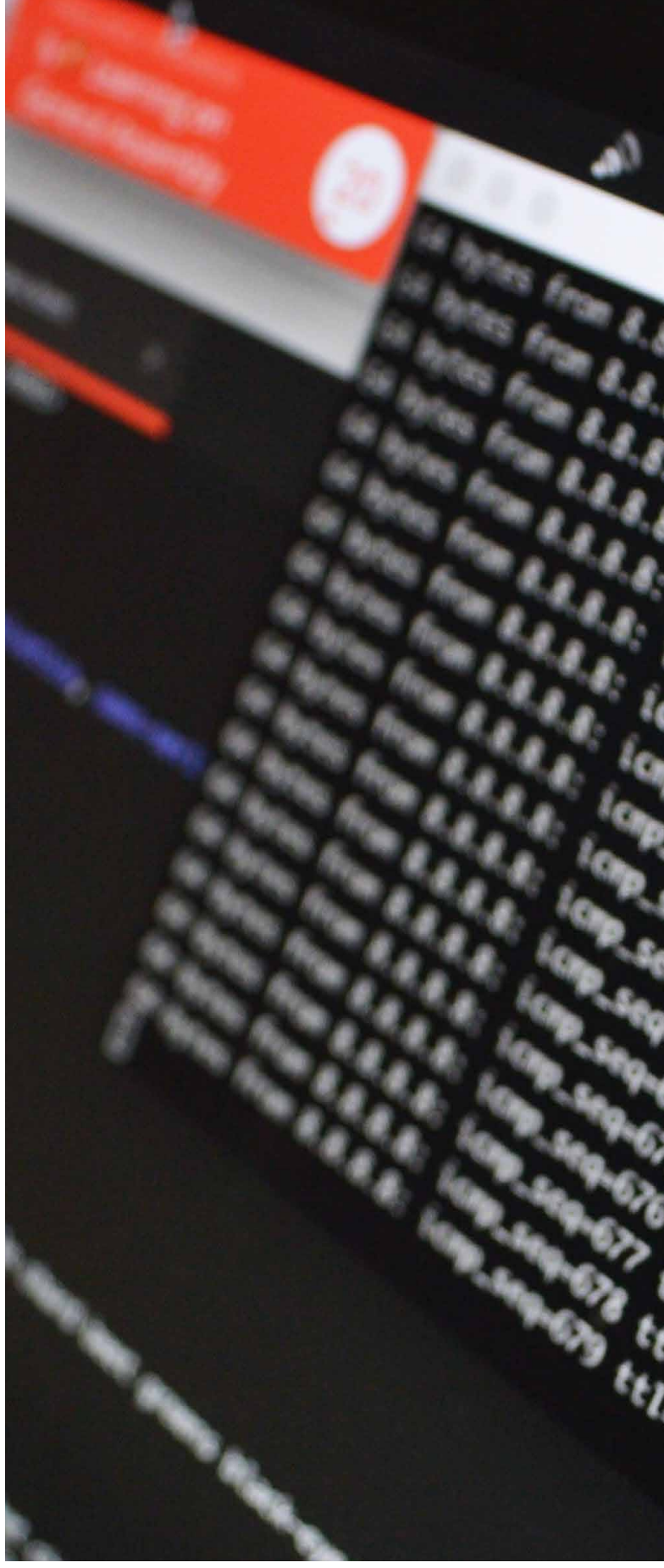
Es crucial proporcionar soporte continuo a los empleados remotos. No espere para proporcionar orientación o recordatorios para la seguridad cibernética. Esta guía contiene recomendaciones prácticas para sus empleados.

A continuación se presentan las estafas prominentes que se están viendo y algunos consejos rápidos para ayudar a su organización a no convertirse en una víctima.

Phishing y Malspam: Recuerde a los empleados que sean cautelosos al abrir correos electrónicos sobre COVID-19, especialmente aquellos de fuera de la organización. Deben tener precaución al ingresar credenciales en un sitio web, vinculadas desde un correo electrónico, mensaje de texto o cuenta de redes sociales, o al descargar archivos adjuntos.

Relleno de credenciales: Puede haber sido necesario poner los servicios a disposición de los empleados de forma remota, sin tiempo para asegurar las cuentas a través de la autenticación multifactor (MFA). Además de proteger las cuentas con MFA, los empleados deben asegurarse de que todas las contraseñas sean seguras y nunca deben reutilizar las contraseñas en diferentes cuentas.

Ransomware: En algunos casos, es posible que los correos electrónicos de malspam que inician una infección de ransomware usen un señuelo COVID-19. Si bien evitar que los ataques de ransomware tengan éxito es el mejor resultado, estar preparado con copias de seguridad es el siguiente mejor.



Orientación del protocolo de escritorio remoto (RDP):

Un aumento en el número de empleados que se conectan de forma remota significa un aumento en el número de sistemas con RDP abierto (puerto 3389) potencialmente escaneados. Si bien su fuerza laboral necesita acceder a los sistemas de forma remota, el acceso limitado y seguro de VPN puede reducir la superficie de ataque.

Ataques distribuidos de denegación de servicio (DDoS):

El tiempo de inactividad de un ataque es aún más perjudicial con una fuerza de trabajo remota. Una fuerza de trabajo remota más grande puede incluso actuar como un ataque DDoS no intencional, simplemente porque más usuarios están intentando acceder a los servicios al mismo tiempo. Para manejar estas posibilidades y garantizar que esté protegido contra ataques DDoS, tenga listas las asignaciones de ancho de banda aumentadas, desactive temporalmente los servicios no utilizados para permitir un mayor ancho de banda y desaliente.

Fuente de información:
https://www.cisecurity.org/

Nuestros especialistas pueden asesorarte.
¡Contáctanos!