Publicado en Madrid el 24/05/2024

Más allá de los ordenadores: los dispositivos cotidianos que se han convertido en el talón de Aquiles de la ciberseguridad empresarial, según Check Point Software

El Brand Phishing Report Q1 2024, muestra un incremento del 5% de los ciberataques con respecto al Q1 de 2023 y un alarmante 28% en comparación con el Q4 de 2023. Check Point Software destaca que los dispositivos IoT, desde impresoras a máquinas de café, enfrentan múltiples vulnerabilidades que comprometen tanto la seguridad de datos personales como corporativos

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder en soluciones de ciberseguridad en la nube basadas en IA, alerta dela peligrosa tendencia que están alcanzando los ciberataques a nivel mundial. Según el Brand Phishing Report Q1 2024, se ha producido un incremento de ciberataques del 5% con respecto al Q1 de 2023 y un alarmante 28% en comparación con el Q4 de 2023.

Las capacidades y optimizaciones que proporciona IoT tanto en el sector de consumo como en el industrial han acelerado su adopción. En 2020, había 9.700 millones de dispositivos IoT desplegados en todo el mundo. Statista estima que para 2030 el número de dispositivos IoT se disparará hasta los 29.000 millones, es decir, prácticamente un 200% más. Dado este importante crecimiento, es crucial evaluar la ciberseguridad de IoT.

Los ciberdelincuentes buscan constantemente puntos débiles dentro de las redes empresariales. Si las empresas no gestionan adecuadamente los dispositivos considerados inofensivos o menos críticos, estos pueden convertirse en vectores de ataque. Desde impresoras hasta máquinas de café, estos aparatos enfrentan múltiples vulnerabilidades que comprometen tanto la seguridad de datos personales como corporativos. Este hecho, junto con la creciente dependencia de estos dispositivos, enfatiza la necesidad de realizar cambios en el ámbito de la ciberseguridad. Check Point Software quiere poner el foco de alerta en algunos de estos aparatos que se descuidan y pueden ser el espía perfecto en cualquier empresa:

Impresoras que pueden ser un espía silencioso: las impresoras multifunción no solo imprimen, sino que también escanean, copian y en muchos casos, envían correos electrónicos o documentos a la nube. Muchas de ellas tienen discos duros internos que almacenan copias de todos los documentos que procesan. Por este motivo, si un ciberdelincuente logra acceder de forma remota a la impresora, podría recuperar estos documentos con información sensible o ser un vector de ataque para alterar configuraciones, o incluso utilizarla como punto de entrada para ataques de mayor alcance. Al igual que con cualquier otro dispositivo conectado a la red, las impresoras multifunción deben mantener al día las actualizaciones de seguridad, cambiar las contraseñas predeterminadas y limitar el acceso a las funciones de red solo a los usuarios necesarios.

Máquinas de café y vending machines inteligentes que pueden hacer algo más que alimentar a los empleados: nadie los considera como una amenaza, pero cada vez están más conectados a Internet para permitir funciones como el pago con tarjeta o el seguimiento en remoto del inventario. La mayoría de las políticas de seguridad TI no consideran estos dispositivos y pueden presentar vulnerabilidades sin parchear o configuraciones débiles por defecto que facilitan el acceso no autorizado. Si estos dispositivos están conectados a la misma red que los dispositivos críticos, podrían ser utilizados como un punto de entrada para ataques de ransomware, especialmente si operan con sistemas operativos conocidos y conectividad a Internet. Para que estén protegidas y no supongan una amenaza para las empresas, es imprescindible segmentarlas en una red separada de los sistemas vulnerables y monitorizar cualquier actividad inusual para poder prevenir cualquier daño a la red.

Teclados y ratones inalámbricos descuidados y omnipresentes: estos dispositivos forman parte de todas las oficinas actuales, pero su comodidad inalámbrica también puede ser explotada. Los atacantes pueden utilizar dispositivos especializados para interceptar las señales inalámbricas enviadas por los mismos, lo que captura cada clic o movimiento del ratón.

Algunos teclados o ratones inalámbricos pueden ser vulnerables a ataques de emparejamiento forzado, donde un atacante fuerza la conexión a un dispositivo no autorizado para capturar entradas o incluso inyectar comandos. No todos los teclados y ratones inalámbricos utilizan cifrado para proteger la transmisión de datos, lo que facilita la tarea de los atacantes para interceptar estas comunicaciones. En este sentido, optar por modelos con cifrado sólido y evitar su uso en entornos donde la seguridad de la información es crítica puede ayudar a mitigar estos riesgos.

Televisores inteligentes, ascensores conectados, sensores, elementos de videovigilancia, etc. Todos estos dispositivos han de ser gestionados adecuadamente para minimizar la superficie de ataque. El control lo se consigue teniendo un inventariado actualizado de todos estos dispositivos, estableciendo y aplicando políticas de conexión, monitorizando y parcheando sus vulnerabilidades, de forma que formen parte de la política integral de seguridad de la compañía.

"El aumento de los ataques contra dispositivos IoT destaca la necesidad de una vigilancia continua y de la implementación de medidas de seguridad más estrictas para proteger estos dispositivos vulnerables" destaca Eusebio Nieva, director técnico de Check Point Software para España y Portugal. "Además de las amenazas habituales, es importante recordar que existen dispositivos que ni siquiera hay que tener en mente, pero que pueden convertirse en puertas de entrada inesperadas. Para hacer frente a esto, es esencial que las empresas adopten un enfoque multifacético de ciberseguridad y aseguren la red mediante tecnologías como la segmentación de redes y firewalls avanzados. También deben comprobar que los dispositivos estén al día con las últimas actualizaciones de seguridad y parches disponibles".

Datos de contacto:
EverythinkPR
EverythinkPR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Nacional Inteligencia Artificial y Robótica Madrid Software Ciberseguridad Oficinas Industria Otras Industrias Innovación Tecnológica Actualidad Empresarial