Silicon.es

23-04-2020

LA OPINIÓN DE LOS EXPERTOS

El teletrabajo en tiempos de COVID-19

Domótica del hogar: ¿qué beneficios y riesgos conlleva?

¿Por qué el cambio de contraseñas obligatorio continuo no es bueno?

Cómo garantizar el teletrabajo seguro en 6 pasos

Reforzar el eslabón débil de la cadena de seguridad de la información

http://tinyurl.com/yc9bt6ag

Silicon.es

23-04-2020

El teletrabajo en tiempos de COVID-19

Emeterio Cuadrado, 23 de abril de 2020, 17:25

SEGURIDAD

Emeterio Cuadrado, director de la Unidad de Seguridad de Grupo CMC, nos ofrece algunos consejos para evitar ser objeto de ciberataques y prácticas cada vez más extendidas por los ciberdelincuentes para aprovecharse de la situación y el estado de alarma en el que nos hallamos inmersos.

La pandemia del COVID-19 nos ha obligado a encerrarnos en nuestras casas y, para muchas empresas, independientemente de su tamaño y actividad, en poco tiempo ha cambiado la forma de seguir desarrollando su actividad. Aunque en muchas organizaciones el teletrabajo venía siendo una práctica habitual, las tecnologías de las que hoy en día disponemos (conexión remota, servicios en cloud, video conferencia y otras herramientas colaborativas) lo han convertido en un método adoptado masivamente como única forma viable de mantener el negocio a flote.

Toda transformación conlleva cambios profundos en la forma en que personas y organizaciones colaboran, y supone, además, importantes retos. Uno de los más significativos es el de la seguridad de la información, de las comunicaciones y de los sistemas. Ante un nuevo escenario como éste, las organizaciones han de responderse a estas cuestiones: ¿A qué nuevas amenazas y riesgos nos enfrentamos? ¿Dónde están ahora nuestras vulnerabilidades? ¿Cómo garantizamos el control de la información de nuestra organización y también de nuestros clientes?

http://tinyurl.com/yc9bt6ag

Silicon.es

23-04-2020

Tres pilares fundamentales ante los nuevos riesgos y amenazas

A medida que el uso de una tecnología se extiende también lo hace el interés de los ciberdelincuentes para buscar y explotar vulnerabilidades, puesto que les permitirá rentabilizar más rápidamente sus esfuerzos. En algunos casos bastará con adaptar algunas técnicas al nuevo contexto. Así, por ejemplo, deberemos estar atentos a nuevas campañas de phishing y suplantación de identidades en las que los delincuentes, haciéndose pasar por personal de soporte o help desk, tratarán de conseguir las credenciales de los usuarios.

En otros casos las nuevas amenazas vendrán de la mano del uso de aplicaciones de comunicación y de las propias herramientas de trabajo colaborativas, que llamarán la atención de los malhechores en búsqueda de nuevas vulnerabilidades y brechas de seguridad.

Las organizaciones deben asegurarse de disponer de una estrategia robusta y global de seguridad para afrontar el nuevo escenario y si no disponen de ella confiar a un tercero experto su definición. Desde Grupo CMC, abordamos este reto basándonos en tres pilares fundamentales: la gestión de identidades, la protección de los datos y la ciberseguridad.

Cómo garantizar el control y la seguridad de la información

Aunque como decimos todos los expertos, el perímetro está cada vez más diluido y centrar la seguridad en su control es una batalla perdida, renunciar a controlarlo es renunciar a utilizar la tecnología de forma segura, por lo que tenemos que vigilar el

que esté bajo nuestra supervisión. Los mayores esfuerzos han de centrarse en controlar, de forma estricta, la gestión de la identidad, asegurando y garantizando los procesos de autenticación (garantizar que las personas son las que dicen ser y no se producen suplantaciones), y autorización (las personas tienen solo y exclusivamente los derechos de acceso que deben tener sobre los sistemas y la información).

Además, este control y derechos de acceso no debe ceñirse exclusivamente a las aplicaciones, sino que debe extenderse a toda la información, a veces no estructurada y de carácter confidencial, que guardan las organizaciones en modo de ficheros y con todo tipo de formatos.

Medidas de seguridad críticas

Si hacemos un repaso detallado de las medidas que, a mi juicio, pueden garantizar el éxito en este proceso, apuntaría como fundamental la revisión de nuestras políticas de passwords para implantar unas más fuertes y un aumento en la frecuencia de cambio por parte de los usuarios. Igualmente, es necesario establecer mecanismos de autenticación de segundo factor para el acceso a sistemas o información especialmente sensibles; así como la realización de una auditoría y revisión de nuestros sistemas de gestión de identidades y accesos para asegurar que todos los usuarios acceden exclusivamente a sus aplicaciones y ficheros.

http://tinyurl.com/yc9bt6ag

Desde que comenzó la crisis, nuestros servicios de gestión de identidades han sido reforzados, y hemos diseñado planes específicos de contingencia por petición expresa de nuestros clientes. Estos sistemas se han vuelto críticos puesto que a través de las herramientas y las plataformas que operamos se provisionan y gestionan los derechos de acceso para que los empleados se conecten y trabajen en remoto.

También es imprescindible disponer de sistemas IRM (Information Rights Management) capaces de proteger toda la documentación sensible y su integración dentro del sistema de gestión de identidades. Hemos comprobado como nuestros clientes del servicio IRM Prot-On en la nube han incrementado el uso de nuestra herramienta de cifrado de documentos para aumentar la seguridad sobre la información confidencial de sus organizaciones. Del mismo modo, la instalación de infraestructuras y servicios para comunicaciones VPN también ha crecido, pasando de una media de una o dos instalaciones al mes a cuatro en una sola semana.

Por otro lado, es recomendable la configuración de los nuevos equipos con las herramientas obligatorias y corporativas para la protección de las máquinas con antivirus y antimalware; así como aumentar la vigilancia y monitorización de los eventos de seguridad a través de sistemas conectados a los firewalls y antivirus de puesto. También es esencial sensibilizar a los usuarios mediante la publicación periódica de información de seguridad y guías de teletrabajo seguro.

Por último, y para redoblar la seguridad, podemos desplegar soluciones CASB (Cloud Access Security Broker) y desarrollar auditorías de Hacking Ético llevadas a cabo por expertos "Red Team" para detectar y analizar vulnerabilidades y brechas de seguridad.

Estos hackers éticos están especializados en el desarrollo de acciones encaminadas a comprometer los activos, tanto informacionales como operaciones de las organizaciones, con el objetivo de identificar debilidades y puntos de mejora. Para ello utilizan prácticas como el "pentesting" o "test de penetración", un ataque dirigido y controlado y otras tan habituales como el lanzamiento de ataques de phishing.

Protección proactiva en cuatro vertientes

En suma, en un modelo de teletrabajo como el actual y con la necesidad de una interconexión total entre empleados y empresas colaboradoras, la ciberseguridad ha de ser comprensiva. Para ello hemos construido soluciones que, combinando tecnología propia y de partners como Fortinet, Nozomi Networks, Empow y SecLab, cubren los requerimientos de seguridad en cuatro vertientes: acceso y movilidad, acceso a datos, seguridad de perímetro, así como los específicos de activos y redes industriales.

En este último ámbito, cabe destacar la potencia de los SIEMs (Security Information and Event Management) de nueva generación que, gracias al uso de Inteligencia Artificial (IA), permiten a los equipos de seguridad avanzar desde una vigilancia reactiva a una vigilancia proactiva, anticipándose a los potenciales ciberataques.

Silicon.es

23-04-2020

En conclusión, y volviendo al principio de estas reflexiones, es previsible que a partir de ahora muchas organizaciones se decidan por el teletrabajo de sus recursos humanos y profesionales por las ventajas evidentes que aporta, pero la única opción es hacerlo eliminando los riesgos aquí descritos y, puesto que la tecnología lo posibilita, tomando posiciones de forma anticipada que nos permitan, con planes concretos de seguridad y análisis de vulnerabilidades de nuestros sistemas, ir por delante de los ciberdelincuentes.

ciberataques coronavirus Grupo CMC pandemia teletrabajo

AUTOR

Emeterio Cuadrado

http://tinyurl.com/yc9bt6ag