Academia de Ingeniería México

RECOMENDACIONES DE LA UIT EN LA EPOCA DEL COVID-19

Debido a la pandemia del COVID-19, se ha generado a nivel mundial el hecho de que el personal de la oficina, los gerentes, los ejecutivos de negocios críticos y el personal administrativo y técnico ahora estén trabajando de forma remota.

La pandemia ha generado una exposición significativa a las amenazas, ya que lo que ayer era una conexión local y segura entre el equipo del usuario y su servidor, hoy contiene un punto de paso adicional, que es la red y los dispositivos domésticos del empleado. Además, se debe considerar como riesgo operativo que la perdida y robo de los dispositivos de acceso remoto, ira en aumento.

A continuación, mencionamos algunos de los requisitos para llevar a cabo las actividades de manera remota.

- Una computadora
- Una buena conexión a Internet
- Aplicaciones de chat para realizar videoconferencia
- Un espacio de trabajo dedicado (deseable)
- Un teléfono (opcional)
- Automotivación y disciplina

Normalmente, cuando un empleado solicita acceso remoto, se le proporciona la capacitación adecuada y los dispositivos con la protección necesaria. Ante la tremenda y súbita demanda de acceso remoto por el COVID-19, es poco probable que se haya aplicado este procedimiento, por lo que la superficie de ataque para los ciberdelincuentes aumenta en proporción al gran número de dispositivos sin seguridad y empleados no capacitados.

Al trabajar desde casa sabemos que las técnicas de suplantación (Phishing), van a ser utilizadas de manera muy agresiva, debido a que el estado de ánimo de los empleados que están trabajando remotamente los hace vulnerables a la ingeniería social, cuya tasa de éxito aumentará seguramente.

Cuando un atacante instala malware, puede hacerse cargo del equipo portátil de un empleado y realizar de forma remota casi cualquier cosa que el empleado esté autorizado a hacer, sin la detección o seguimiento del área de auditoría.

Recomendaciones.

- Aplicar un enfoque basado en el riesgo para hacer el mejor uso de los recursos que pudieran ser escasos.
- Identificar como prioridad, a los empleados con acceso a la información más sensible, las funciones comerciales de mayor riesgo y las relacionadas con el dinero.
- Utilizar perfiles basados en roles y privilegios mínimos para limitar los derechos de acceso, sobre todo para administradores con credenciales de alto nivel.
- Eliminar los derechos de administrador local de las cuentas de empleados que se usan a diario. Esto limitara drásticamente lo que un atacante pueda hacer.

- Los canales de comunicación deben estar fuertemente cifrados, ya que los accesos remotos deben considerarse como de riesgo alto y medio.
- La autenticación simple basada en contraseña es insuficiente. Se necesita autenticación de dos factores.
- Para empleados como ejecutivos, administradores y tomadores de decisiones, se recomienda la autenticación de dos factores. (Tokens)
- Para los empleados restantes, utilice adicionalmente un mecanismo de verificación de texto SMS a un dispositivo móvil pre-registrado.
- Es fundamental la supervisión de toda la actividad del canal de acceso remoto en base a patrones de actividad de los empleados, buscando anomalías que nos indiquen una credencial comprometida.
- Las herramientas para la prevención de pérdida de datos, se pueden utilizar para supervisar el tráfico de salida en busca de datos confidenciales y propietarios.

Muchas otras medidas de seguridad son necesarias para formar un entorno de protección completo.

- El acceso remoto solo se debe permitir desde una dirección IP registrada "lista blanca" y desde un portátil registrado con "dirección MAC".
- Utilice únicamente dispositivos de acceso remoto para funciones de trabajo y no para internet.
- Aplique contraseñas seguras en el arranque de su equipo y establezca tiempos para la suspensión del equipo por inactividad.
- La impresión de documentos debe ser controlada.
- Los datos de los dispositivos de acceso remoto deben cifrarse.
- Utilice siempre una VPN para conectar trabajadores remotos a la red interna de la organización.
- Controle el uso de dispositivos externos, como los de almacenamiento USB, así como dispositivos periféricos.
- Limite la capacidad de almacenar, descargar o copiar datos.
- Se recomienda la utilización de una aplicación de monitoreo en la red doméstica.
- La capacidad de destrucción remota puede ayudar a gestionar el aumento de la pérdida y el robo del dispositivo.
- Los dispositivos de acceso remoto deben utilizarse en privado y protegidos físicamente cuando no estén en uso.

- Comparta una lista con los contactos útiles de soporte técnico. De esta manera los trabajadores remotos sabrán con quien comunicarse cuando sea necesario.
- Sería prudente hacer un repaso de concientización sobre seguridad informática, para ayudar a evitar el error humano que los ciberdelincuentes tanto intentan explotar.

Documento de referencia: UIT by Jacques Francoeur, Chief Scientist and Founder at Security Inclusion Now USA

A mi me encuentran en Twitter en @jfniembro

Y les invito a seguir a Pedro Ferriz de Con en Centralfmonline.com