PERIÓDICO	PAGINA	FECHA	SECCIÓN
EXCELSIOR	1,6	07/10/2022	LEGISLATIVO

SEDENA ALERTÓ A SU PERSONAL DE RIESGOS

Videos porno y juegos abren puerta a hackers

BAJAR CONTENIDO riesgoso, compartir contraseñas y usar correos gratuitos para tratar asuntos confidenciales son prácticas entre militares que causan fuga de datos

Guacamaya #LEAKS

POR ANDRÉS MENDOZA

El mal uso del servicio de internet en instalaciones militares facilita los ciberataques contra la Secretaría de la Defensa Nacional (Sedena), alertó la propia institución.

Un reporte contenido en la información hackeada por Guacamaya detalla malas prácticas en las que incurre personal castrense, que "propician fugas de información".

"Se visitan sitios web con contenido pornográfico o para la descarga gratuita de programas, lo cual propicia que los sistemas operativos se contaminen con códigos maliciosos, afectando su desempeño y exponiendo la seguridad de la información", alerta el documento.

Bajar programas de entretenimiento es otro problema, pues "degradan el funcionamiento del sistema e incluso deshabilitan los mecanismos de seguridad (antivirus, firewall, antiespías)".

El informe destaca que las organizaciones delictivas pueden aprovecharse de que los equipos conectados a internet son empleados para publicar información de las instalaciones, operaciones y del personal militar.

Otras malas prácticas son el uso de cuentas de email gratuito (Hotmail, Yahoo, Gmail) para comunicar información oficial. Además, personal castrense comparte contraseñas y, sin autorización, habilita redes inalámbricas con acceso a internet.

PRIMERA | PÁGINA 6

PERIÓDICO	PAGINA	FECHA	SECCIÓN
EXCELSIOR	1,6	07/10/2022	LEGISLATIVO

REVELAN DESCUIDOS DE MILITARES

Videojuegos y porno dieron paso a hackers

ENTRE LAS DIEZ MALAS PRÁCTICAS están que los equipos de cómputo carecen de antivirus, descarga de programas de entretenimiento y uso de mail gratuito para comunicar información oficial

POR ANDRÉS MENDOZA
amendoza@gimm.com.mx

En cuestiones de ciberseguridad, la Secretaría de la Defensa Nacional también tiene a un enemigo en casa.

Un reporte de este año hallado por **Excélsior** en la información sustraída por el grupo de hacktivistas Guacamaya enlista diez malas prácticas en las que incurre personal castrense al usar el servicio de internet en instalaciones militares.

Estas acciones "han propiciado fugas de información", reconoce el informe interno, y van desde la descarga de juegos al uso de cuentas gratuitas de correo electrónico para compartir información confidencial, pasando por el empleo de equipos sin herramientas de seguridad instaladas.

Además, "se visitan sitios web con contenido pornográfico o para la descarga gratuita de programas, lo cual propicia que los sistemas operativos se contaminen con códigos maliciosos, afectando su desempeño y exponiendo la seguridad de la información", alerta el inciso F del informe.

La descarga de programas de entretenimiento es otro problema, pues de acuerdo con la Sedena "automáticamente degradan el funcionamiento del sistema e incluso deshabilitan los mecanismos de seguridad (antivirus, firewall, antiespías)".

En el inciso E se advierte el uso de equipos de cómputo que carecen de antivirus o sus sistemas operativos no están actualizados "siendo objetivos para la sustracción de información confidencial."

El informe destaca que organizaciones delictivas pueden aprovecharse de que los equipos conectados a internet son empleados para publicar abiertamente información de las instalaciones, operaciones y del personal militar.

La ciberseguridad también se compromete porque a las instalaciones militares se introducen, sin permiso, dispositivos para la recepción de señal de internet, como antenas y tarjetas USB de banda ancha. Otra mala práctica es que se utilizan cuentas de correo electrónico gratuito (hotmail, yahoo, gmail, entre otros servicios) para comunicar información oficial. Los militares emplean dispositivos de su propiedad sin que existan controles de acceso y salida de las instalaciones militares.

El riesgo de sustracción de datos se incrementa porque en horas no laborables, se permite que se alterne la conexión a internet con equipos que resguardan información militar y que carecen de medidas de seguridad adecuadas.

Además, personal castrense comparte contraseñas o habilitar redes inalámbricas con acceso a internet sin la autorización correspondiente.

"Algunas redes de cómputo con conexiones físicas o inalámbricas, previamente autorizadas, conectan más equipos de los autorizados, compartiendo la contraseña o deshabilitando los mecanismos de seguridad para facilitar el acceso a internet, percibiéndose que en algunos casos esto se hace para sufragar el costo del servicio", indica el reporte.

PERIÓDICO	PAGINA	FECHA	SECCIÓN
EXCELSIOR	1,6	07/10/2022	LEGISLATIVO

El diputado Javier López Casarín y los senadores Ricardo Monreal y Jorge Carlos Ramírez Marín.

Foto: Especial

EL DATO

Poca seguridad

A las instalaciones se introducen, sin permiso, dispositivos para la recepción de señal de internet, como antenas y tarjetas USB de banda ancha.

Conectan más equipos de los autorizados, compartiendo la contraseña o deshabilitando los mecanismos de seguridad para facilitar el acceso a internet."

INFORME

EL DATO

Advertencia

En horas no laborables, se permite que se altere la conexión a internet con equipos que resguardan información militar y que carecen de medidas de seguridad adecuadas, lo que incrementa el riesgo de sustracción de información.

SE INFORMA A USTED QUE SE CONTINUAN OBSERVANDO DEFICIENCIAS Y OMISIONES EN EL EMPLEO DEL SERVICIO DE INTERNET EN LAS INSTALACIONES MILITARES, LAS CUALES HAN PROPICIADO FUGAS DE INFORMACIÓN, DESTACANDO LOS CASOS SIGUIENTES:

A. SE HABILITAN REDES INALÁMBRICAS CON ACCESO A INTERNET SIN LA AUTORIZACIÓN CORRESPONDIENTE.

B. ALGUNAS REDES DE CÓMPUTO CON CONEXIONES FÍSICAS O INALÁMBRICAS PREVIAMENTE AUTORIZADAS POR EL SUSCRITO, CONECTAN MÁS EQUIPOS DE LOS AUTORIZADOS, COMPARTIENDO LA CONTRASEÑA O DESHABILITANDO LOS MECANISMOS DE SEGURIDAD PARA FACILITAR EL ACCESO A INTERNET, PERCIBIÉNDOSE QUE EN ALGUNOS CASOS ESTO SE HACE PARA SUFRAGAR EL COSTO DEL SERVICIO.

C. EN HORAS NO LABORABLES, SE PERMITE QUE SE ALTERNE LA CONEXIÓN A INTERNET CON EQUIPOS QUE RESGUARDAN INFORMACIÓN MILITAR Y QUE CARECEN DE MEDIDAS DE SEGURIDAD ADECUADAS, LO QUE INCREMENTA EL RIESGO DE SUSTRACCIÓN DE INFORMACIÓN.

D. SE INSTALAN PROGRAMAS DE ENTRETENIMIENTO GRATUITOS QUE AUTOMÁTICAMENTE DEGRADAN EL FUNCIONAMIENTO DEL SISTEMA E INCLUSO DESHABILITAN LOS MECANISMOS DE SEGURIDAD (ANTIVIRUS, FIREWALL, ANTI ESPÍAS).

E. SE OBSERVAN EQUIPOS DE CÓMPUTO QUE CARECEN DE LAS HERRAMIENTAS DE SEGURIDAD (ANTIVIRUS, FIREWALL, ANTI ESPÍAS Y ACTUALIZACIONES DEL SISTEMA OPERATIVO), SIENDO OBJETIVOS PARA LA SUSTRACCIÓN DE INFORMACIÓN CONFIDENCIAL.

F. SE VISITAN SITIOS WEB CON CONTENIDO PORNOGRÁFICO O PARA LA DESCARGA GRATUITA DE PROGRAMAS, LO CUAL PROPICIA QUE LOS SISTEMAS OPERATIVOS SE CONTAMINEN CON CÓDIGOS MALICIOSOS, AFECTANDO SU DESEMPEÑO Y EXPONIENDO LA SEGURIDAD DE LA INFORMACIÓN.

G. LOS EQUIPOS CONECTADOS A INTERNET SON EMPLEADOS PARA PUBLICAR ABIERTAMENTE INFORMACIÓN DE LAS INSTALACIONES, OPERACIONES Y DEL PERSONAL MILITAR, LA CUAL PUEDE SER EMPLEADA Y EXPLOTADA POR ORGANIZACIONES DELICTIVAS.

H. SE EMPLEAN EQUIPOS PROPIEDAD DEL PERSONAL MILITAR, SIN QUE EXISTA EL CONTROL DE ACCESO Y SALIDA DE LAS INSTALACIONES MILITARES.

I. SE INTRODUCEN SIN AUTORIZACIÓN A LAS INSTALACIONES MILITARES, DISPOSITIVOS PARA LA RECEPCIÓN DE SEÑAL DE INTERNET (TARJETAS USB DE BANDA ANCHA Y ANTENAS).

J. SE UTILIZAN CUENTAS DE CORREO ELECTRÓNICO GRATUITO (hotmail, yahoo, gmail, otros) PARA COMUNICAR INFORMACIÓN OFICIAL.