Ransomware: Una amenaza digital que secuestra datos

El ransomware es un tipo de software malicioso o malware que cifra los datos del usuario o bloquea el acceso a sistemas informáticos, exigiendo un pago o «rescate» para restaurar el acceso o descifrar la información. El término «ransomware» proviene de la combinación de las palabras «ransom» (rescate) y «software».

Cómo afecta a las organizaciones:

1. Pérdida de Acceso y Datos: Una vez que el ransom

wa
re
in
fe
ct
a
un
si
st
em
a,
pu
ed
e
ci
fr
ar
ar
ch
iv
os
va
li
os
os
,
ba
se
s
de
da
to
s
y
ap
li
ca

ci
on
es
,
ha
ci
en
do
qu
e
es
to
s
se
an
in
ac
ce
si
bl
es
pa
ra
la
or
ga
ni
za
ci
ón
.

2. Costo Económico: Más allá del rescate que los atacantes puedan exigir, las organizaciones enfrentan costos asociados a la interrupción de sus operaciones, la recuperación de datos (si es posible), la contratación de expertos en ciberseguridad y posibles sanciones legales.

3. Reputación Dañada: Un ataque de ransomware puede dañar gravemente la confianza de clientes, socios y stakeholders, quienes podrían cuestionar la capacidad de la organización para proteger información sensible.

4. Consecuencias Legales: Dependiendo de la jurisdicción y la naturaleza de los datos comprometidos, las organizaciones pueden enfrentar sanciones legales por no proteger adecuadamente la información de sus clientes o usuarios.

5. Tiempo de Inactividad: A medida que los equipos de TI luchan para recuperar sistemas y datos, las operaciones normales pueden verse interrumpidas, lo que puede resultar en pérdidas significativas, especialmente para aquellas empresas que dependen en gran medida de sistemas en línea.

6. Presión Psicológica y Toma de Decisiones: Las organizaciones afectadas enfrentan la difícil decisión de pagar o no el rescate. Pagar puede parecer una solución rápida, pero no garantiza la recuperación de datos y puede alentar a los ciberdelincuentes a seguir atacando.

Concretando un poco, el ransomware no es solo un problema técnico, sino que presenta desafíos multifacéticos para las organizaciones, afectando su operatividad, finanzas, reputación y, en ocasiones, su continuidad en el mercado.

Reacciones Inmediatas ante un Ataque de Ransomware

Las primeras horas después de un ataque de ransomware son cruciales para determin

ar
la
gr
av
ed
ad
de
l
in
ci
de
nt
e
y
to
ma
r
me
di
da
s
pa
ra
mi
ti
ga
r
su
s
ef
ec
to
s.
Aq
uí
ha
y

un
re
su
me
n
de
la
s
re
ac
ci
on
es
tí
pi
ca
s
qu
e
un
a
or
ga
ni
za
ci
ón
po
dr
ía
te
ne
r
al
en
fr
en

ta
r
ta
l
si
tu
ac
ió
n:

Detección y Confirmación:

El reconocimiento oportuno de un ataque de ransomware es esencial para mitigar sus efectos. Los primeros momentos son cruciales, y entender los indicadores de compromiso puede ayudar a confirmar la presencia del ransomware. A continuación, se detallan los pasos y signos a tener en cuenta:

1. Síntomas Visibles:

– Notas de Rescate: A menudo, una de las primeras señales es una nota de rescate que aparece en el escritorio o en directorios con archivos cifrados. Esta nota usualmente contiene detalles sobre el cifrado y cómo realizar un pago para obtener la clave de descifrado.

– Extensiones de Archivos Cambiadas: Los archivos pueden haber cambiado su extensión a algo inusual o desconocido, indicando que han sido cifrados.

2. Performance del Sistema:

– Lentitud: Un ataque de ransomware en progreso puede ralentizar un sistema debido al proceso de cifrado de archivos.

– Programas y Archivos Inaccesibles: Aplicaciones que no se inician o documentos que no se abren, indicando que han

sido comprometidos o cifrados.

3. Alertas de Herramientas de Seguridad:

– Las soluciones de seguridad, como antivirus o sistemas de detección de intrusiones, pueden generar alertas sobre actividades sospechosas o la presencia de software malicioso.

4. Monitoreo de Red:

– Un aumento inusual en el tráfico de red puede ser un indicador de que datos están siendo cifrados o exfiltrados.

5. Validación con Usuarios y Personal de TI:

– A menudo, los usuarios pueden ser los primeros en notar comportamientos extraños en sus sistemas. Es vital establecer una comunicación rápida con ellos para confirmar los síntomas.

6. Análisis Forense:

– Usar herramientas especializadas para analizar el comportamiento y la naturaleza del código malicioso.

– Identificar el tipo específico de ransomware, lo que puede ayudar a determinar sus capacidades, intenciones y posibles soluciones.

7. Revisión de Logs y Registros:

– Consultar registros de eventos del sistema y logs de aplicaciones para identificar patrones anómalos o entradas sospechosas que puedan indicar una infección.

8. Validación de Backups:

– Verificar si las copias de seguridad también han sido afectadas o cifradas por el ransomware.

9. Confirmación del Ataque:

– Una vez que se han recopilado suficientes evidencias y

se ha identificado el comportamiento característico del ransomware, se puede confirmar con certeza el ataque.

Una vez confirmado el ataque de ransomware, es esencial proceder rápidamente con las siguientes etapas de respuesta para contener y mitigar el daño. Esta fase inicial de detección y confirmación es fundamental para informar y orientar las acciones subsecuentes.

Aislamiento del Sistema ante un Ataque de Ransomware

El aislamiento es una de las primeras y más críticas re

sp
ue
st
as
de
sp
ué
s
de
de
te
ct
ar
un
at
aq
ue
de
ra
ns
om
wa
re
.
Su
ob
je
ti
vo
pr
in
ci
pa
l
es
co
nt

en
er
la
pr
op
ag
ac
ió
n
de
l
ma
lw
ar
e
y
pr
ot
eg
er
si
st
em
as
y
da
to
s
no
af
ec
ta
do
s.
A
co
nt

in
ua
ci
ón
,
se
de
ta
ll
a
có
mo
ll
ev
ar
a
ca
bo
el
ai
sl
am
ie
nt
o:

1. Desconectar de la Red:

– Desconecte físicamente las máquinas afectadas de la red, ya sea desenchufando cables Ethernet o desactivando adaptadores inalámbricos.

– Si el ransomware está en una red corporativa, considere desconectar segmentos enteros de la red o aislar VLANs sospechosas.

2. Apagar Servicios y Protocolos de Red:

– Desactive servicios y protocolos no esenciales, como el intercambio de archivos, RDP (Remote Desktop Protocol) y otros servicios de acceso remoto.

– Estos protocolos pueden ser vías que el ransomware utilice para propagarse.

3. Desactivar Cuentas Comprometidas:

– Si se identifica que cuentas específicas están siendo utilizadas para propagar el ransomware, estas cuentas deben ser desactivadas inmediatamente.

4. Aislamiento de Sistemas de Backup:

– Asegúrese de que las copias de seguridad, especialmente aquellas no afectadas, estén aisladas y desconectadas. Esto previene que el ransomware cifre o dañe estos valiosos recursos.

5. Aislar Dispositivos Móviles y Remotos:

– Si los empleados tienen acceso remoto o usan dispositivos móviles conectados a la red corporativa, es crucial comunicarles que desconecten y no accedan hasta nuevo aviso.

6. Monitoreo Activo de la Red:

– Utilice herramientas de monitoreo y detección de intrusiones para observar el tráfico y las actividades en la red. Esto ayuda a identificar cualquier intento de movimiento lateral por parte del ransomware.

7. Limitar Accesos a Internet:

– Bloquee el tráfico a sitios web y servidores asociados con el ransomware, si se han identificado. Esto puede prevenir la comunicación del malware con sus servidores de comando y control.

8. Mantener Comunicación Segura:

— Establezca canales de comunicación seguros y confiables con el equipo de respuesta a incidentes, el personal de TI y otros stakeholders clave. La información deberá ser compartida rápidamente, pero de manera segura.

9. Evaluación y Cuarentena:

— Analice sistemas y dispositivos para identificar signos de infección. Los sistemas sospechosos deben ser puestos en cuarentena para su posterior análisis y limpieza.

10. Documentación:

— Mantenga un registro de todas las acciones tomadas durante el proceso de aislamiento. Esta documentación será esencial para investigaciones posteriores y posibles medidas legales.

Una vez que el sistema o la red esté adecuadamente aislada, el siguiente paso será la evaluación detallada del daño, la recuperación de datos y la implementación de medidas de seguridad mejoradas para prevenir futuros ataques.

Notificación Interna ante un Ataque de Ransomware

Una comunicación interna efectiva y oportuna es esencial después de detectar un at

aq
ue
de
ra
ns
om
wa
re
.
Es
cr
uc
ia
l
qu
e
to
da
s
la
s
pa
rt
es
re
le
va
nt
es
de
nt
ro
de
la
or
ga
ni

za
ci
ón
es
té
n
in
fo
rm
ad
as
y
al
in
ea
da
s
pa
ra
co
or
di
na
r
un
a
re
sp
ue
st
a
ad
ec
ua
da
.
Aq

uí
te
pr
es
en
to
un
es
qu
em
a
de
có
mo
pr
oc
ed
er
co
n
la
no
ti
fi
ca
ci
ón
in
te
rn
a:

1. Equipo Directivo:

– Qué: Informe inmediato sobre la detección del incidente, la magnitud percibida y las acciones iniciales tomadas.

– Por qué: La alta dirección necesita estar informada para

tomar decisiones estratégicas, asignar recursos y estar preparada para comunicaciones externas.

2. Equipo de Respuesta a Incidentes:

– Qué: Detalles técnicos del incidente, sistemas afectados, tipo de ransomware detectado, etc.

– Por qué: Este equipo liderará la respuesta técnica al incidente y comenzará el proceso de contención, erradicación y recuperación.

3. Departamento de TI y Seguridad:

– Qué: Información sobre el ataque, sistemas comprometidos y directrices sobre pasos a seguir.

– Por qué: Estos equipos desempeñarán un papel vital en el aislamiento, análisis y recuperación del incidente.

4. Comunicación y Relaciones Públicas:

– Qué: Descripción general del incidente y la posible repercusión para preparar declaraciones y gestionar las comunicaciones externas.

– Por qué: Anticipar preguntas de los medios, stakeholders y público en general y preparar respuestas coherentes y transparentes.

5. Departamento Legal:

– Qué: Detalles sobre la naturaleza y magnitud del incidente.

– Por qué: Evaluar las implicaciones legales, posibles responsabilidades y guiar la organización en aspectos regulatorios y legales.

6. Recursos Humanos:

– Qué: Información general sobre el incidente y cómo puede afectar las operaciones diarias y a los empleados.

– Por qué: Gestionar posibles inquietudes de los empleados y ayudar en la comunicación interna a nivel de toda la organización.

7. Todos los Empleados:

– Qué: Comunicado breve sobre el incidente, recomendaciones iniciales (por ejemplo, no abrir correos sospechosos, guardar su trabajo, etc.) y la promesa de actualizaciones regulares.

– Por qué: Para mantener a todos informados, reducir el pánico y garantizar que se sigan las medidas de precaución.

8. Documentación:

– Mantener un registro detallado de todas las comunicaciones enviadas, con fechas, horas y destinatarios.

– Por qué: Esto es esencial para la revisión posterior del incidente y posibles investigaciones.

9. Actualizaciones Regulares:

– Proveer actualizaciones regulares a todas las partes relevantes a medida que se desarrolla la situación y se obtiene más información.

– Por qué: Mantener a todos informados y alineados es esencial para una respuesta organizada y efectiva.

Una comunicación interna adecuada no solo asegura una respuesta coordinada al incidente, sino que también ayuda a mantener la confianza dentro de la organización y a reducir el pánico y la desinformación.

IFX, una empresa con negocios en Colombia, fue víctima de un ataque de ransomware el 12 y 13 de septiembre de 2023. El ataque, que se cree que fue llevado a cabo por un grupo de

hackers conocido como BlackMatter, paralizó las operaciones de la empresa, incluyendo sus sistemas informáticos, redes y servidores.

Esta noticia, dadas sus consecuencias en grandes entidades e instituciones del Estado, nos hizo reflexionar y empezar está secuencia de post relacionados, con la intención de aprender y extraer la mayor cantidad de moralejas posibles al respecto, dado que la seguridad web siempre es un riesgo en mayor o menor medida para las empresas online.

Leer también: Backup remoto, qué es y porqué es importante; Almacenamiento remoto; Veeam cloud backup ; Cómo prevenir un ataque de ransomware video