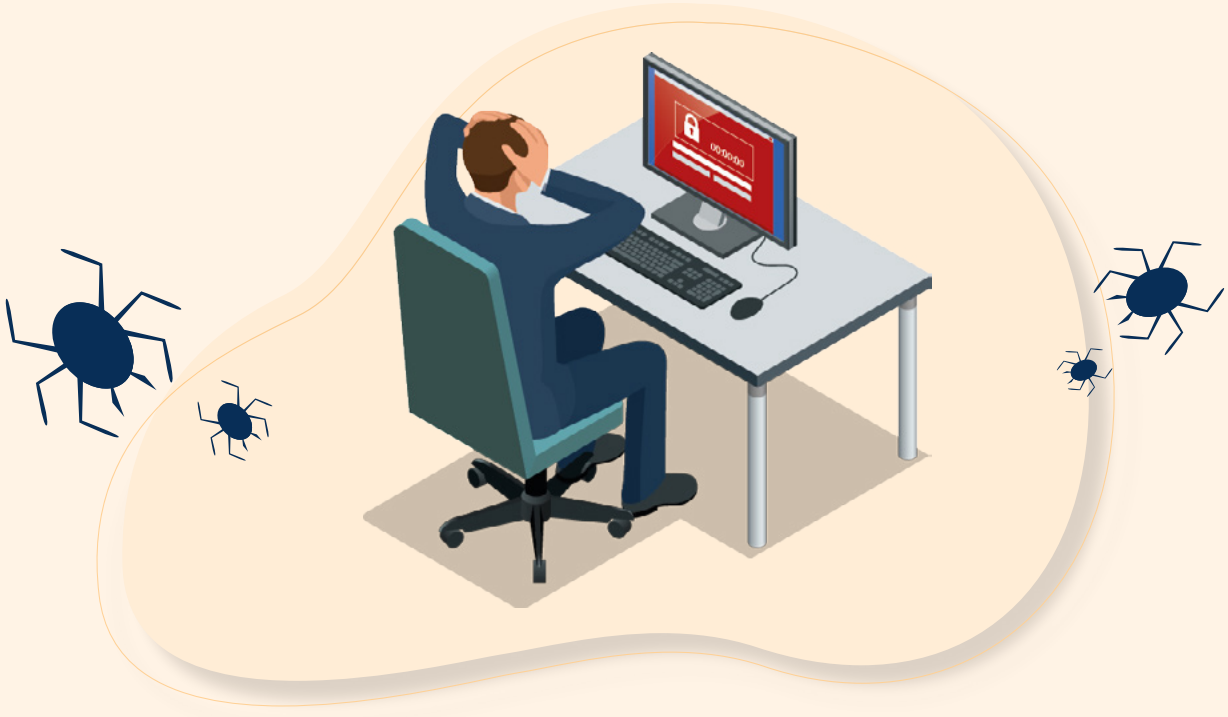
CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

10th anniversary EUROPEAN CYBER SECURITY MONTH

PREVENCIÓ I RESPOSTA PER A ATACS DE RANSOMWARE



En aquest document, trobarà un protocol per a previndre i respondre als atacs de ransomware i tindre la seua empresa preparada per a aquestes amenaces cibernètiques.

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Fons Europeu de Desenvolupament Regional
Una manera de fer Europa
UNIÓ EUROPEA

Actuació susceptible de ser cofinançada per la Unió Europea a través del Programa Operatiu del Fons Europeu de Desenvolupament Regional (FEDER) de la Comunitat Valenciana 2014-2020

PREVENCIÓ

Previndre un atac de ransomware

1. Dispositius de programari

- Supervise que tots els usuaris inicien sessió i treballen des d'una VPN.
- Assegure's de tindre un tallafoc instal·lat i funcionant activament.
- La seua organització ha d'aplicar actualitzacions i mesures de protecció d'endpoint. També es poden combinar amb llistes blanques, bloqueig d'executables en temps real, etc.
- Cree un sistema antispam/antiphishing dedicat, siga mitjançant programari o utilitzant els dispositius de maquinari dedicat.
- El procediment de pegats dins de la seua organització ha de ser molt disciplinat i les actualitzacions han d'aplicar-se a totes les aplicacions i al sistema operatiu, tan prompte com es detecten les vulnerabilitats i isca un nou pegat.
- Utilitze tècniques de seguretat de correu electrònic d'avantguarda com DNSSEC, DANE, SPF, DKIM.

2. Solucions de còpia

- Implemente una solució de còpia de seguretat sofisticada per a les dades de la seua organització, siga basada en programari o basada en maquinari, o fins i tot una combinació d'ambdues.
- Realitze proves periòdiques tant de les seues funcions de recuperació (quan es tracta de la seua solució de còpia de seguretat) com de les seues dades en general. Totes les dades fins uns quants mesos abans han de provar-se regularment per a garantir que no es vegen compromesos des de dins mentre ocorre l'atac.
- Verifique si la seua solució de còpia de seguretat cobreix totes les seues dades, per a assegurar-se que totes es guarden i s'hi puga accedir en cas que ocórrega el pitjor.
- També és important que les seues dades recolzades siguen fàcilment accessibles en la seua forma de suport, i que les seues dades estiguen segures en general. Seguisca el principi 3-2-1: tinga tres còpies de seguretat diferents, en dos tipus diferents de mitjans i mantinga una còpia de seguretat fora del lloc.

3. Mètodes de prevenció de robatori

- Aprofite els registres del sistema per a realitzar un seguiment dels moviments de dades.
- Implemente tecnologies d'encriptació de dades per a les seues dades en general.
- Adquirisca i utilitze àmplies eines de DLP (prevenció de fugida de dades).
- No oblide analitzar el trànsit de la seua xarxa, per a buscar moviments de dades inusuals dins del sistema.
- Utilitze el mètode de permisos mínims per a protegir les seues bases de dades, carpetes i arxius singulars (això significa que no atorgue als seus usuaris cap permís a part dels que necessiten per a fer el seu treball correctament).

4. Coneixement dels usuaris

- Simule regularment atacs de phishing per a educar els seus usuaris sobre el protocol d'acció a seguir, així com per a provar els seus propis sistemes.
- Invertisca en capacitació de conscienciació sobre seguretat per als seus usuaris, perquè sàpien com buscar aplicacions sospitoses i no descarregar-les/executar-les.
- Establisca una línia d'informes i un flux de treball clars i fàcils de seguir per a informar sobre incidents sospitosos. Faça que els seus usuaris ho sàpien!

RESPOSTA

Respondre a un atac de ransomware.

1. Desconnecte la font del ransomware

- El seu primer pas sempre ha de ser limitar l'escala de l'atac tant com siga possible, i això significa que ha de:
    - Desendollar totes les computadores afectades de la xarxa.
    - Apagar tots els mètodes sense fils de transmissió de dades, inclosos Bluetooth, Wi-Fi, NFC, etc.
    - Identificar tots els dispositius que hagen sigut compromesos.

2. Determinar l'escala de l'atac

- Immediatament després d'intentar limitar l'abast de l'atac, és essencial esbrinar l'escala del mal fins al moment, cosa que significa buscar signes d'encriptació inusual dins de diferents ubicacions d'emmagatzematge, com ara:
    - Unitats de disc dur.
    - Ubicacions d'emmagatzematge basades en el núvol (OneDrive, DropBox, Google Drive, etc.).
    - Unitats assignades o compartides.
    - Diferents dispositius d'emmagatzematge USB, com unitats USB, càmeres/telèfons connectats, etc.
    - Diversos dispositius d'emmagatzematge en xarxa.

Cride a les agències locals de llei/policia/CERT. En alguns casos, això pot fins i tot ser un requisit legal. A més, l'anàlisi forense necessària a partir d'aquest moment probablement estarà per damunt del que fins i tot el seu equip d'administració pot fer.

3. Esbrine si alguna de les seues dades ha sigut robada

- Hi ha diferents mètodes per a fer-ho, que inclouen:
    - En general, una de les indicacions més òbvies de robatori de dades és algun tipus de notificació dels atacants cibernètics que les seues dades han sigut robades.
    - Arxius inusualment grans amb format d'arxiu (.zip, .7z, etc.) que contenen dades confidencials transmeses a través de la seua xarxa.
    - Els registres i els informes del programari DLP poden ajudar a trobar signes de fugides de dades en alguna part.

És possible que puga trobar el malware o les eines que es van usar per a la infecció.

LLISTA DE CONTROL

Què ha de revisar en cas de patir un atac de ransomware en la seua organització:

Llista de control

1. Restaure els seus arxius des d'una còpia de seguretat

- Assegure's que s'elimine el vector d'atac inicial perquè no torne a ser atacat.
- Localitze les seues còpies de seguretat i assegure's que contenen tots els arxius.
- Verifique la integritat de les seues còpies de seguretat i busque signes de corrupció.
- També es recomana buscar instantànies (si és possible) i versions anteriors dels seus arxius (si es tracta d'emmagatzematge en el núvol).
- Restaure els seus arxius recolzats.
- Descobrisca el vector d'infecció i com tancar-lo.

2. Si està intentant desxifrar els seus arxius

Això es pot intentar principalment en casos específics quan és possible determinar el tipus de ransomware i hi ha un desencriptador disponible per a aquest cep específic.

- Per a desxifrar els seus arxius, en cas d'haver localitzat un desencriptador, només ha de connectar tots els mitjans d'emmagatzematge que s'han vist afectats pel ransomware.
- Descobrisca el vector d'infecció i com tancar-lo.

3. Si no fa res respecte al ransomware

- És possible que considere fer una còpia de seguretat dels seus arxius encriptats i no eliminar-los, per si més endavant hi haguera un desencriptador per a aquest cep específic.

CSIRT-CV

Centre Seguretat TIC de la Comunitat Valenciana

10th anniversary EUROPEAN CYBER SECURITY MONTH

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

Fons Europeu de Desenvolupament Regional
Una manera de fer Europa
UNIÓ EUROPEA

Actuació susceptible de ser cofinançada per la Unió Europea a través del Programa Operatiu del Fons Europeu de Desenvolupament Regional (FEDER) de la Comunitat Valenciana 2014-2020