COMUNICAT DE L'INCIDENT DE "RANSOMWARE" a APARCAMENTS MUNICIPALS DE TARRAGONA S.A

PREVI

En data 12 de febrer els i les treballadores d'APARCAMENTS MUNICIPALS DE TARRAGONA S.A (d'ara en endavant AMT), van comprovar que un dels servidors informàtics de l'empresa no carregava el sistema operatiu i no iniciava la seva activitat, conforme això els equips interns i externs d'informàtica varen iniciar el protocol de recuperació i d'incidents informàtics concloent que hi havia diversos fitxers xifrats i un document HTML on s'indicava un correu electrònic i la referència "RYUK".

El "RYUK" es un virus de rescat i xantatge de la família "ransomware", en que el seu sistema d'afectació consisteix en xifrar els fitxers de la màquina o hardware on s'executa i les que hi pugui tenir accés, dades que no s'exporten del mitjà infectat però deixa les bases inaccessibles.

El sistema de rescat consisteix en comunicar amb el correu electrònic que faciliten els arxius i un cop comunicats i previ pagament de "rescat", és facilitat un codi que permet accedir als arxius on hi ha les dades encriptades.

Dels tres servidors tots afectats el més preocupant es el AMTSASERVER, en que hi ha la majoria de bases de dades de l'empresa.

ACTUACIONS LEGALMENT ESTABLERTES:

En data 14 de febrer de 2019, es va donar compte a l'empresa externa responsable de protecció de dades de caràcter personal i al comitè de compliance de les empreses municipals de Tarragona, de l'incident que s'havia patit.

La responsable externa de protecció de dades, va procedir a l'estudi de la situació i incident i va determinar des de les obligacions establertes en la llei i el reglament de protecció de dades de caràcter personal, en especial l'art. 33 RGPD, que s'havia de procedir conforme al protocol establert per les anomenades esquerdes de seguretat, en no disposar AMT de signatura digital per l'afectació patida als servidors, la comunicació a les autoritats responsables de protecció de dades, va ser efectuada des de l'empresa externa el mateix dia 14 de febrer de 2020 i per tant dins del termini legalment establert, comunicació amb el número de registre 007150/2020.

Els experts externs per determinar la comunicació de la bretxa de seguretat van realitzar l'avaluació segons indicacions de l'AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES resultant una afectació de 30 punts, (nombre de dades afectades, sensibilitat de les dades i impacte), conforme aquesta avaluació la decisió legalment establerta era la de comunicar la bretxa a les autoritats i procedir a la denúncia penal, però sense la necessitat de comunicació a les persones afectades.

En data 13 de febrer de 2020 el Gerent d'AMT informa dels fets als MMEE, amb la informació rebuda per MMEE i segons les instruccions rebudes de la Gerència d'AMT i conforme a protocols, es va procedir a denunciar els fets a la policia MMEE el 15 de febrer de 2020, mitjançant compareixença personal.

ALTRES ACTUACIONS

TÈCNICO INFORMÀTIQUES

1. Informàtiques o tècniques realitzades

1.1. Recuperar MV centraleta telefònica

1.1.1. Migració de servidor antic a nou

1.2. Disposar de 2 controladors de domini

1.2.1. instal·lació nova MV amb DC principal

1.2.2. Instal·lació nova MV amb DC secundari

1.3. dades no afectades des de backup

1.3.1. Recuperació fixers (carpetes compartides)

1.3.1.1. Recuperar fitxers sobre el DC principal

1.3.2. Recuperació SAGE

1.3.2.1. instal·lació nova MV per SAGE

1.3.2.2. Recuperació dades SAGE antic

1.3.3. Recuperació FITXADOR

1.3.3.1. instal·lació nova MV per FITXADOR

1.3.3.2. Recuperació dades FITXADOR antic

1.4. Netejar/reinstal·lar equips d'usuari

1.4.1. Reintegrar equips en domini

1.5. Implementar noves eines de seguretat

- Implantació de nou disseny de sistema de còpies de seguretat per entorn de virtualització, per protecció de servidors o Solució: Veem Backup & Replication v10

Beneficis: protecció de servidors virtuals, disponibilitat d'agents específics per serveis concrets: SQL Server

- o Notes: versió gratuïta fins 10 MV, ampliable amb llicències addicionals

- Disseny directives d'usuari per facilitar la centralització de dades en servidors i no en els equips d'usuari, per facilitar la seva protecció

- Revisió solució antivirus i estudi de possibles millores/funcionalitat

TÈCNICO JURÍDIQUES

S'ha efectuat informe i s'ha certificat per part del president de l'associació de pèrits judicials ASPERTIC, que no hi ha hagut tràfic de sortida de dades ni d'informació encriptada o no d'AMT a l'exterior, afirmant-se i certificant-se, després d'anàlisi forense que no es va produir cap fugida de dades.

CONCLUSIONS

Conforme a tot l'anterior hem de concloure, que si be APARCAMENTS MUNICIPALS DE TARRAGONA S.A va patir un atac de ransomware conegut com a "RYUK", provenint aquest atac d'un correu electrònic d'un proveïdor habitual, en que l'atacant va camuflar el seu atac, infectant els servidors D'AMT, especialment facturació i part de les bases de dades dels clients.

La bretxa de seguretat no ha suposat en cap cas, la migració de dades, ni consta que s'hagi pogut accedir a les dades personals que disposem, per part dels atacants, sinó que aquestes han quedat segrestades a demanda d'un rescat que evidentment ens hem negat a pagar.

Els fets han estat posat en coneixement de les autoritats policials i judicials, en coneixement de les autoritats administratives de protecció de dades, s'han complert els protocols legalment establerts i s'ha realitzat una comunicació pública, a més s'han realitzat per tècnics informàtics no només les revisions i neteja dels sistemes, sinó que s'estan implementant noves i més estrictes normes de seguretat per evitar cassos com el què malauradament hem viscut, seguim treballant per millora ri per això ens hem posat en mans de perits judicials per tal de que realitzin els informes i seguiment degut.

La única afectació als nostres clients, és que ens han de tornar a lliurar les seves dades, per continuar amb la relació que ens vincula.

Lamentem les molèsties i sensació de vulnerabilitat que aquesta situació hagi pogut ocasionar a tots els nostres clients i col·laboradors, però us volem transmetre un missatge de tranquil·litat i de seguretat de que hem actuat degudament i que en cap cas les vostres dades, han estat sostretes ni facilitades a tercers, havent realitzar anàlisi forense de tots els sistemes i els informes per especialistes que segueixen constantment l'inicident .

Restem a la vostra disposició per qualsevol consulta, que podeu dirigir a Sra. Cecilia Mangini cmangini@aparcamentstgn.cat on atendrem els vostres dubtes i qüestions relacionades amb aquest incident.

Atentament

Tarragona 1 Abril de 2020.

Vocal Extern CEPRAN Òrgan de Vigilància i Control GERÈNCIA