



P5. MODEL DE NEGOCI

PROCÉS DE CANVI EN UNA ORGANITZACIÓ

PQTM 19. TÈCNIC/A EN CIBERSEGURETAT

Joan Santacana - jsantacana@uoc.edu

Ivan Ricart - iricartb@uoc.edu

Khalid Dhabí - kdhabi@uoc.edu



PROCÉS DE CANVI EN UNA ORGANITZACIÓ

1. DESCRIPCIÓ DE L'ESCENARI
2. MECANISMES UTILITZATS PER DETECTAR LES NECESSITATS
3. LLISTA PRIORITZADA DE CANVIS A REALITZAR
4. ESTIMACIÓ ECONÒMICA
5. PLA DE GESTIÓ DEL CANVI
6. AMORTITZACIÓ
7. MONITORITZACIÓ



2. DETECCIÓ DE NECESSITATS

2.1. ÚS DE L'EINA PILAR ESTANDARDITZADA PER MAGERIT

- IDENTIFICACIÓ I VALORACIÓ D'ACTIUS
- IDENTIFICACIÓ I VALORACIÓ DE LES AMENACES
- IDENTIFICACIÓ DE LES SALVAGUARDES O CONTROLS
- VALORACIÓ DELS IMPACTES I NIVELL DE RISC

2.2. ENTREVISTES AMB EL PERSONAL DE L'ORGANITZACIÓ

- ANALITZAR LES TASQUES
- INTERACCIÓ AMB EL PROGRAMARI
- ESTUDI DE VULNERABILITATS
- AMENACES MATERIALITZADES AL LLARG DEL TEMPS ► “EXPERIÈNCIES”

2.1. DETECCIÓ DE NECESSITATS - PILAR



PILAR v7.3.3 - Realització d'un anàlisi de riscos mitjançant la identificació i valoració dels actius, identificació i valoració de les amenaces (freqüència d'ocurrència, percentatge de degradació), identificació dels salvaguardes o controls, valoració dels impactes i el nivell de risc.

ACTIUS

- PLATAFORMA D'ENSENYAMENT ON-LINE
- SALA DE SERVIDORS / EQUIPS
- SERVEI D'ACCÉS ALS FITXERS EN XARXA
- CORREU ELECTRÒNIC EXTERNALITZAT
- ...
- PERSONAL ENC. DE LA GESTIÓ / ENSENYAMENT

CLASSIFICACIÓ AMENACES

- [N] DESASTRES NATURALS
- [I] D'ORIGEN INDUSTRIAL
- [E] ERRORS I FALLES NO INTENCIONADES
- [A] ATACS INTENCIONATS

2.1. DETECCIÓ DE NECESSITATS - PILAR



SERVEIS INTERNS	AMENACES	SALVAGUARDES / CONTROLS
[IS_MDL] Ens. On-Line	[I.5] Avaria física o lògica [E.20] Vulnerabilitats en els programes [E.21] Errors de mant. / Act. (sw) ... [A.24] Denegació del servei	[SW.CM.3] Seguiment d'actualitzacions [SW.CM.a] Control versions act. (sw) [SW.CM.e] Proves en equips aïllats ... [SW.CM.e] Protecció atacs DoS * Fa ús d'una estratègia "hot site" amb Abocament sincronitzat (dades sincronitzades entre els 2 centres)

2.1. DETECCIÓ DE NECESSITATS - PILAR



SALA DE SERVIDORS	AMENACES	SALVAGUARDES / CONTROLS
[HW_SRV_VOIP] [HW_SRV_AD] [HW_SRV_WEB] [HW_SRV_SQL] [HW_SRV_BKP] [HW_SRV_OTR]	[N.1] Focs [N.2] Danys per aigua [N.*] Desastres naturals [I.3] Contaminació mediambiental [I.5] Avaria física o lògica [I.7] Temperatura o humitat [E.2] Errors del administrador [E.23] Errors de mant. / Act. (hw) ... [A.11] <u>Accés no autoritzat</u>	[L.6.2.c] Detecció d'incendis [L.6.3.4] Detecció d'inundacions [L.6.5] Protecció cont. mediambiental [HW.CM.3] Rec. del fabricant [HW.CM.4] Seguiment d'actualitzacions ... [PPS.8] <u>Control de claus</u> (insuficient) ▶ Pèrdua, Duplicitat, etc. <hr/> [Dispositius Biomètrics]
INSTAL·LACIONS (GEN.)	AMENACES	SALVAGUARDES / CONTROLS
Equips, projectors, etc.	[A.11] <u>Accés no autoritzat</u>	[PPS.8] <u>Control de claus</u> (insuficient) <hr/> [Dispositius Biomètrics]

2.1. DETECCIÓ DE NECESSITATS - PILAR



SERVEIS INTERNS	AMENACES	SALVAGUARDES / CONTROLS
[IS_FS] Fitxers en Xarxa	[I.5] Avaria física o lògica [E.19] Fugues d'informació [E.20] Vulnerabilitats en els programes [E.21] Errors de mant. / Act. (sw) [A.15] <u>Modificació delib. Informació</u> ▶ Ransomware ... [A.24] Denegació del servei	[SW.CM.3] Seguiment d'actualitzacions [PS.AT] Formació i conscienciació ... [H.Tools.AV] <u>Antivirus</u> (insuficient) ▶ Desactualització, Ineficàcia, etc. [SW.A] <u>Copies de seguretat</u> <hr/> [NGFW - Next Generation Firewall]
SERVEIS EXTERNS	AMENACES	SALVAGUARDES / CONTROLS
[IS_MAIL] E-Mail	[A.8] Difusió de software perillós ... [A.*] Atacs de Phishing	[H.Tools.AV] <u>Antivirus</u> (insuficient) ▶ Desactualització, Ineficàcia, etc. <hr/> [NGFW - Next Generation Firewall]

2.2. DETECCIÓ DE NECESSITATS - ENTREVISTES



ENTREVISTES - S'han realitzat diverses entrevistes sobre el personal de l'organització per analitzar les seves tasques, la interacció amb el programari, les possibles vulnerabilitats i les amenaces materialitzades al llarg del temps.

Hem detectat que falten coneixement de ciberseguretat en l'àrea TIC. ▶ **Grup de Treball**

El personal encarregat de la gestió, enregistra amb paper i seguint un format predeterminat, les sol·licituds de les claus per accedir a les diverses zones de les instal·lacions, especificant el nom de la persona que ho sol·licita, la data / hora de recollida i de retorn i la signatura.

Ens han comentat, basada en la seva experiència, que més d'un cop s'han perdut les claus / targetes RFID per accedir a les instal·lacions i que algun cop la persona que ha retornat les claus no ha correspost amb la persona que les ha sol·licitat. ▶ **Dispositius Biomètrics**

També ens han comentat, que l'any passat van sofrir un atac de Phishing i que una empleada va executar un programa maliciós d'aquesta web falsificada que va provocar la encriptació de totes les dades emmagatzemades en el servidor de fitxers. ▶ **Next Generation Firewall**

3. CANVIS A REALITZAR



3.1. CREAR UN GRUP DE TREBALL DE CIBERSEGURETAT DINS DE L'ÀREA TIC

3.2. MODIFICAR LA SEGURETAT DE CONTROL DE TRÀFIC ACTUAL

- DISPOSITIU NGFW ► EVITAR EL SOFTWARE MALICIÓS, ATACS DE PHISHING, ETC.

3.3. MODIFICAR EL MECANISME D'ACCÈS FÍSIC A LES INSTAL·LACIONS

- DISPOSITIU BIOMÈTRIC ► EVITAR L'ACCÈS NO AUTORITZAT

3.4. MODIFICAR EL MECANISME D'ACCÉS A LA INFORMACIÓ CENTRALITZADA

- CANVIAR LES UNITATS MAPEJADES PER ENLLAÇOS ► MINIMITZAR IMPACTE RANSOMWARE

3.5. IMPLEMENTAR UNA EINA DE ESCANEIG DE VULNERABILITATS CENTRALITZAT

- ESCANEIG DE VULNERABILITATS ► MILLORA CONTINUA DE LA SEGURETAT

3.3. CANVIS A REALITZAR - ACCÉS FÍSIC



SAMSUNG SHP-DP728 - CARACTERÍSTIQUES

- AUTENTICACIÓ BLUETOOTH, FINGERPRINT, RFID CARDS, PASSCODE
- SHOME MOBILE APP - AUTH & REAL-TIME DOOR EVENTS
- DETECCIÓ DE MOVIMENTS SOSPITOSOS MITJANÇANT SENSORS IR
- PERMET DOBLE VERIFICACIÓ, PIN + FINGERPRINT
- VIDA DE LA BATERIA ~ 10 MESOS
- ALTES PRESTACIONS, INTEGRITAT, ELEGÀNCIA I ECONÒMIC
- COST 450 - 550 €
- COMPARACIÓ MARCA SUPREMA
 - FALTA INTEGRACIÓ ▶ LECTOR + CONTROLADORA
 - POCA ELEGÀNCIA I PRESTACIONS, LECTOR BE PLUS 2 ~ 800 €



3.3. CANVIS A REALITZAR - ACCÉS FÍSIC



SAMSUNG SHP-DP728 - PROCEDIMENT

- INSTAL·LAR DISPOSITIUS
- ENREGISTRAR EMPREMPTES DACTILAR
- CONFIGURAR PERMISOS / ROLS
- 5 DISPOSITIUS EN PRODUCCIÓ
 - ENTRADA PRINCIPAL A LES INSTAL·LACIONS ▶ **ROLS / EMPLEATS**
 - DIRECCIÓ ▶ **ROLS / EMPLEATS ENC. DIRECCIÓ**
 - GESTIÓ / ADMISTRACIÓ ▶ **ROLS / EMPLEATS ENC. GESTIÓ**
 - SALA DE SERVIDORS ▶ **ROLS / IT**
 - SALA DE REUNIONS ▶ **ROLS / EMPLEATS**
- 1 DISPOSITIU EN RESERVA



3.4. CANVIS A REALITZAR - ACCÉS INFORMACIÓ



ACCÉS INFORMACIÓ - CARACTERÍSTIQUES I PROCEDIMENT

- INTRODUIR UNA NOVA CAPA DE PROTECCIÓ
 - FIREWALL ▶ SI NO DETECTA L'AMENAÇA ▶ PROTECCIÓ INFERIOR
 - ANTIVIRUS ▶ SI NO DETECTA L'AMENAÇA ▶ PROTECCIÓ INFERIOR
- CANVIAR LES UNITATS MAPEJADES PER ACCESSOS DIRECTES
- MINIMITZAR L'IMPACTE DELS VIRUS RANSOMWARE
 - ATAQUEN L'ACTIU MÉS IMPORTANT ▶ INFORMACIÓ
 - ANALITZEN LES UNITATS PER ENCRIPAR MÉS INFORMACIÓ
 - ENGANYAR EL COMPORTAMENT MITJANÇANT ENLLAÇOS LNK
 - COMPORTAMENTS MÉS COMPLEXOS ▶ FALLIDA DE LA CAPA
- FACILITAT D'IMPLANTACIÓ I BAIX COST



7. MONITORITZACIÓ



NEXT GENERATION FIREWALL

- UTILITZAR LA PLATAFORMA WEB DEL SERVIDOR WEB ► INFORMES
- INFORMES MENSUALS / AMENACES DETECTADES / IP'S ATACANTS RECURRENTS / ETC.

DISPOSITUS BIOMÈTRICS

- UTILITZAR LA PLATAFORMA WEB DEL SERVIDOR WEB ► INFORMES
- INFORMES MENSUALS / ACCESSOS ERRONIS ► EFECTIVITAT DELS MEC. DE AUTENTICACIÓ

ESCANEIG DE VULNERABILITATS

- UTILITZAR LA PLATAFORMA WEB DEL SERVIDOR WEB ► INFORMES
- INFORMES MENSUALS D'ESCANEIG DE LA XARXA / VULNERABILITATS DETECTADES