SANTÉ & BIOMÉDICAL : ET LA SÉCURITÉ DANS TOUT CA ?

TREND MICRO

CONSTAT

1 200 appareils biomédicaux infectés dans les hôpitaux britanniques en 2017

Source : ARS Pays de la Loire

58% des hôpitaux font une priorité de l'accès aux données du SI clinique à des fins d'analyse et de reporting

Source : Observatoire Santé IDC, 2017

RENSEIGNEMENTS PERSONNELS SUR LA SANTÉ : PRINCIPALES DONNÉES ENVOYÉES DEPUIS DES INFRASTRUCTURES :

28%	E-MAILS
23%	TERMES MÉDICAUX
18%	NOMS
14%	DIAGNOSTIQUES
6%	MÉDICAMENTS
4%	NUMÉROS DE TELÉPHONE
4%	DATE DE NAISSANCE, ÂGE, SEXE
3%	NUMÉRO DE SÉCURITÉ SOCIALE

Etude réalisée par Trend Micro aux Etats-Unis et au Canada

PRINCIPAUX SYSTÈMES DE SANTÉ EXPOSÉS

- Appareils connectés à Internet exposant des systèmes de Dossier de Santé Electronique (DSE)
- Appareils non sécurisés
- Protocoles de Remote Desktop
- Systèmes de Contrôle Industriels (ICS)
- Outils de communication et autres vulnérabilités en ligne

DIRECTIVES

- **Instruction 309**
  Plan d'action SSI à 6, 12 et 18 mois
- **Instruction 340**
  Plan de sécurisation des ES avec volet cyber ciblant le biomédical
- **Hop'EN**

E-SANTÉ : UN SECTEUR EN TRANSFORMATION

ROBOTIQUE BIOMÉDICAL · TÉLÉMÉDECINE · TÉLÉSANTÉ · M-SANTÉ · OBJETS CONNECTÉS · DATA ANALYSE

MENACES

PRINCIPAUX RISQUES

- Attaques ciblant les logiciels intégrés aux équipements
- Compromission du site web, du Dossier de Santé Electronique (DSE) ou du portail interne
- Menaces émanant des équipes internes ou des fournisseurs de l'établissement hospitalier
- Prestataires externes
- Compromission des applications de santé mobiles
- Compromission des codes source lors de la fabrication
- Hameçonnage (Spear Phishing) utilisant des adresses email de confiance

DONNÉES EXPLOITÉES PAR LES CYBERCRIMINELS AU SEIN DES DOSSIERS DE SANTÉ ÉLECTRONIQUES (DSE) :

- Approvisionnement de médicaments
- Vols d'identité
- Numéros d'assurance maladie
- Certificats de naissance
- Déclarations de revenus erronées

PRINCIPAUX IMPACTS DES ATTAQUES CIBLANT LES DISPOSITIFS BIOMÉDICAUX :

- Prise en charge et vie privée des patients
- Organisation des soins
- Image de l'établissement hospitalier
- Pertes financières
- Pénalités ou amendes (réglementations, GDPR, lois nationales spécifiques)
- Perte d'avantage concurrentiel
- Mesures de remédiation techniques et non techniques
- Soucis juridiques

PÉRIMÈTRE DE CIBLES

GTB
IRM
Scanner
Frigo connecté
Automates de biologie
Couveuses connectées
Pompes à morphine
Gestion des flux d'air
Contrôles d'accès
...

SÉCURISER LE PARCOURS DE SOIN & PROTÉGER LES ENVIRONNEMENTS BIOMÉDICAUX

COMMENT SE PRÉMUNIR ?

- **Evaluer les vulnérabilités** des nouveaux équipements médicaux
- **Instaurer un système d'authentification** NAC avant d'autoriser l'accès au réseau dans le cadre des programmes de BYOD
- **Investir dans des équipements médicaux** conçus par des acteurs appliquant des règles de sécurité rigoureuses lors de la conception et de la fabrication
- **Développer une stratégie de patch et de mise à jour** des codes et logiciels intégrés aux dispositifs implantés chez les patients ou aux équipements médicaux en place dans les établissements hospitaliers
- **Evaluer les risques** liés à l'ensemble des fournisseurs et prestataires externes au sein de la chaîne logistique et vérifier les antécédents des employés ayant accès aux équipements médicaux
- **Effectuer des tests de sécurité, de vulnérabilité et d'intrusion** au sein du réseau et des applications de l'établissement hospitalier afin de s'assurer que ces derniers sont protégés contre les hackers

ACCOMPAGNEMENT SÉCURITÉ & OUTILS DE PROTECTION :

- Dispositifs antimalware
- Maintenance des signatures antivirales
- Accès au support logiciel/matériel
- Documentation administrateur et guide d'utilisation en Français
- Synthèse des points de vigilance sur le paramétrage et l'utilisation
- Webinaire d'accompagnement
- Réunion de bilan et retours d'expérience 1 an après

BÉNÉFICES :

- Sensibiliser aux risques
- Décloisonner les équipes biomédicales et SI
- Améliorer la détection des malware
- Ouvrir le dialogue

TREND MICRO PORTABLE SECURITY

ROUGE :
Scan des malware terminé. Détection d´un malware et attente d´une action.

VERT :
Scan des malware terminé. Détection d´un malware et nettoyage de celui-ci.

BLEU :
Scan des malware terminé. Aucun malware détecté.

Analyse antivirale et restauration pour les terminaux hors ligne

- Pas d'installation de logiciel requise sur l'appareil
- Simplicité d'utilisation
- Gestion centralisée

POUR ALLER PLUS LOIN

www.trendmicro.fr

Vos contacts santé :
Région Nord :
yannick_boucard@trendmicro.com
Région Sud :
christophe_cothenet@trendmicro.com