proximus NXT
cybersecurity

Cyberweek 2023 : la cybersécurité dans le secteur de la santé
Retours d'expérience et tour d'horizon

10/2023

antonio.paci@proximus.com

Cybersecurité dans le secteur de la santé, ou en suis-je ?

Cybersecurity, les bonnes pratiques
Step 1: d'abord bien se connaître

1

- Etude de l'infrastructure et des applications
- Etude de la sécurité existante
- Evaluation des risques spécifiques aux métiers
- Identification des vulnérabilités non couvertes
- Etude de la réglementation applicable
- Leçons tirées des incidents
- Evaluation des capacités de recouvrement

Bien connaître la situation présente

2

- Prévention, Détection, Réaction, Recouvrement
- Amélioration des systèmes en place
- Installation des composants complémentaires
- Définition des services attendus
- Définition du partage des rôles et responsabilités
- Etablissement d'un plan d'évolution à long terme

Etablir la meilleure stratégie

3

- Choix des technologies, des constructeurs et leur forme
- Fixer le niveau de partage de services interne/ externe
- Choix du modèle de financement capex / opex
- Evolutions de l'infra et de la sécurité envisagées à court terme
- Déterminer les "quick-wins"

Choisir la tactique la plus appropriée

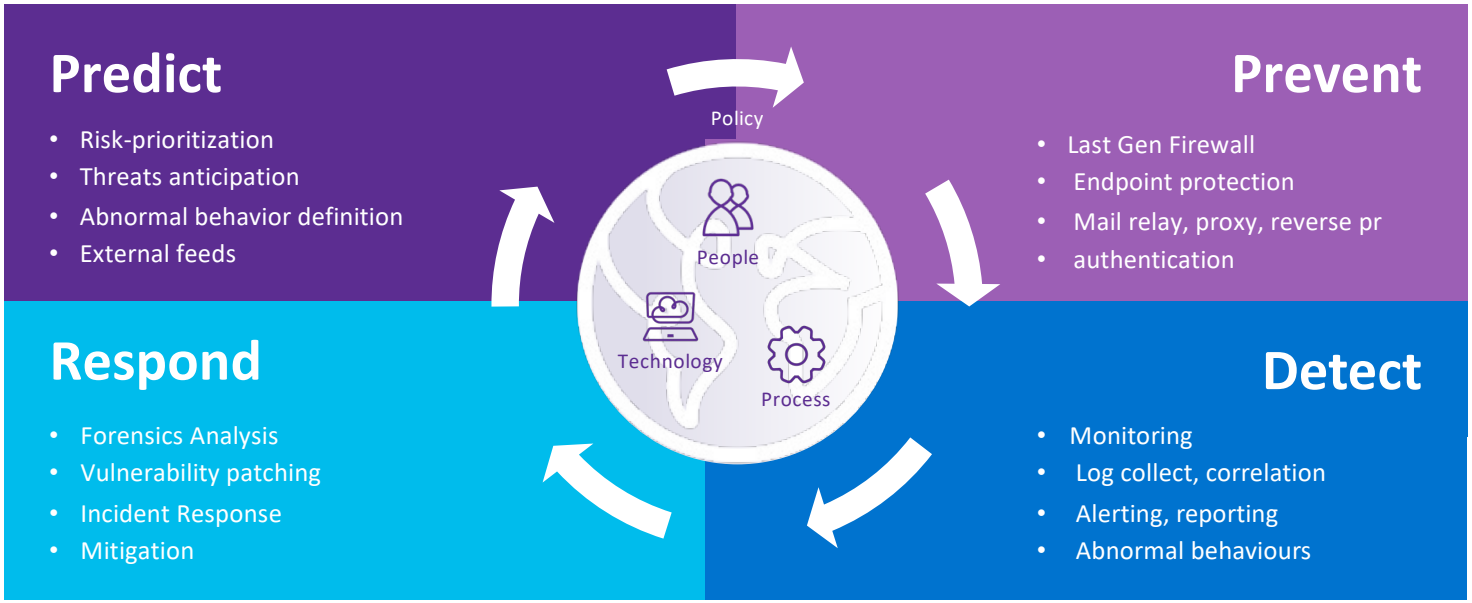
4

- Calcul budgétaire pour la maintenance de l'existant, et la couvertaure des nouveaux risques
- Choix des constructeurs les plus adéquats (eco-system)
- Définition des services d'installation et maintenance
- Choix de la période contractuelle

Décider du meilleur modèle de financement

Quelles sont les spécificités du secteur de la santé ?
Assez peu, tout compte fait …

- Le secteur est large: prévention, diagnostic, traitement, gestion, recherche, administration, pharma, biotech, hôpitaux, assurance maladie, sécurité sociale,… Les profiles sont variés, les risques sont différents, la législation est spécifique mais les fondements de la cyber protection sont toujours les mêmes.



Quels sont les spécificités Cyber dans le secteur de la santé ? Le retour d'expérience

Les hôpitaux sont devenus des cibles aussi attrayantes que les autres mais avec des points faibles bien connus des pirates:

- Les nouvelles surfaces d'attaque spécifiques liées aux machines médicales
- Les machines des collaborateurs externes (BYOD ?)
- Les échanges de données avec les sytèmes extérieures et les sous-traitants
- Les vulnérabilités négligées
- Le stress lié aux conséquences possibles sur l'intégrité physique des personnes
- Le sous financement et le manque de politique commune liés à l'organisation de ce secteur en Be.

Les réponses aux questions

- Sur qui puis-je compter en cas d'attaque ?

Le CSIRT est composé de l'équipe IT interne, assistée par des experts externes appelables sur demande. Les "premiers soins" consistent à comprendre l'attaque afin de décider des mesures de confinement. Cette étude passe par l'analyse des traces (logs) et des images des machines infectées. L'efficacité sur CSIRT repose sur une bonne preparation: comment isoler un incident, identifier la cause, éradiquer la menace, restaurer à partir des sauvegardes fiables*, appliquer les correctifs et comment gérer la crise

- Suis-je vulnérable au ransomware ?

Ici le cycle complet prévention, détection et réaction joue son rôle. D'abord par un contrôle du traffic entrant par la messagerie, ensuite par le contrôle du traffic entrant par le surf et enfin, par la protection antimalware active sur la machine. Au delà de ces composants, des tests de phishing participent à éduquer les utilisateurs et à tester le système en place

Les réponses aux questions

- Suis-je suffisamment résilient ?

La continuité des services doit être assurée quel que soit le type et l'ampleur de l'attaque. Elle repose sur des éléments essentiels comme la détection précoce des premiers signes, la réaction automatisée, un design agile, des procédures de backups fiables et un plan de continuité,… La resilience évite les baculements intempestifs en mode DRP.

- Comment reconstruire après une attaque ?

Les backups et plan de continuité de services intégrent les attaques cyber comme tout autre incident de la vie réelle. La continuité et la fiabilité des procédures de backups sont monitorées, testées et améliorées régulièrement. Une analyse détaillée de tous les événements survenus avant, pendant et après un sinistre permet de tirer des enseignements. Ceci demande une tracabilité compléte conservée pendant une période de temps suffisante.

Les réponses aux questions

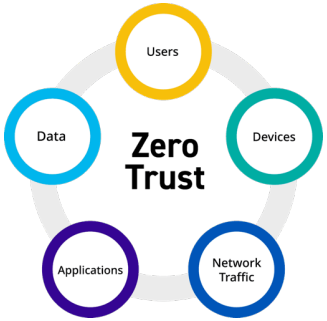
- Suis-je conforme au GDPR ?

Le sujet ne se réduit pas à la sécurité opérationelle. Mais si nous l'examinons sous le prisme de la sécurité des données, le GDPR demande de protéger les données personnelles contre la perte, le vol, l'accès non autorisé et la divulgation. En bref, se protéger de tout ce qui peut alétérer, détruire ou voler les données sensibles. Les réponses sont multiples et passent par la mise en oeuvre de contrôle d'identité renforcé et continu pour les machines, les utilisateurs, les applications pour les données en transit ou les données stockées complétée par une tracabilité de bout en bout.

Remarque

Le domaine devient très large et très complexe. Les experts manquent. Un bon partage des rôles est absolument nécessaire entre l'équipe IT interne et les prestataires externes. L'automatisation des déploiements et des réactions aux incidents est aujourd'hui possible (et l'AI en fait partie). Ceci procure une détection plus fine et un temps de réaction plus rapide.

La checklist du secteur santé



- Network Segmentation (Data / Medical devices / Servers / Communication / Safety / …)
- Access Control: strong authentication for all
- Network firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) for North-South & East-West
- Regular Software Patching and Updates
- Endpoint Detection & Response on the workstations & on the servers onsite or in the cloud
- Data Encryption of sensitive information in transit and at rest
- Employee Training and Awareness
- Incident Response Plan: logging, monitoring, detecting, alerting, reporting, mitigating & reaction to cybersecurity incidents.
- Vendor and Third-Party Risk Management
- Medical Device Security
- Data Backup, Recovery & Business Continuity Plan
- Security Audits, Pentesting and Assessments
- Legal and Regulatory Compliancy
- Physical Security interfacing (?)

Cybersecurity is an ongoing process
requiring continuous monitoring, assessment, and
adaptation to address evolving threats and vulnerabilities.

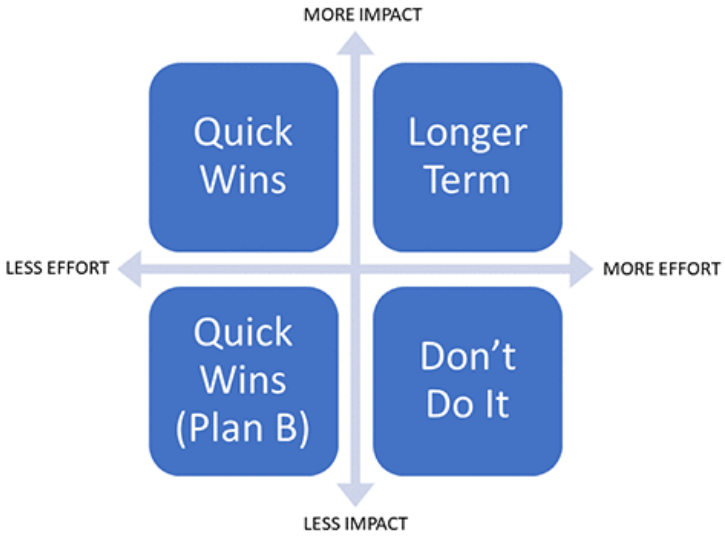
Cybersecurity, steps to success
Regulations, what is mandatory or recommended

CENTRE FOR CYBER SECURITY BELGIUM

- GDPR
- CCB NIST CSF, ISO 27001 / ISO 27002, CIS Controls and IEC 62443
- A hospital is considered as “Essentials” following CCB
- (https://ccb.belgium.be/en/cyberfundamentals-framework)
- Reco’s classified by category: Identify, Protect, Detect, Respond & Recover
- Services: Threat Intell Platform, Safeonweb, Csirt, Vulnerability scaning

Cybersecurity
Des exemples de “Quick Wins”

- ✓ Multi Factor Authentication pour tous les users
  (PR.AC-1;PR.AC-3;PR.AC-4;PR.AC-6;PR.MA-2)
- ✓ Endpoint Detection & Response sur toutes les machines
  (ID.AM-2;PR.DS-1;PR.MA-2;PR.PT-2;PR.PT-3;DE.CM-3;DE.CM-4)
- ✓ Conscientisation des utilisateurs
  (PR.AT-1;PR-AT-5;RC.IM-1)
- ✓ Data backup
  (PR.IP-4)
- ✓ Mises à jour logiciels
  (PR.MA-1)



Cybersecurity, steps to success
Services in governance & operations

- Presales
- Consultancy
- Solution Setup
- Migration, transition
- Maintenance operations
- Cybersecurity operations
- Assessment
- Governance assistance

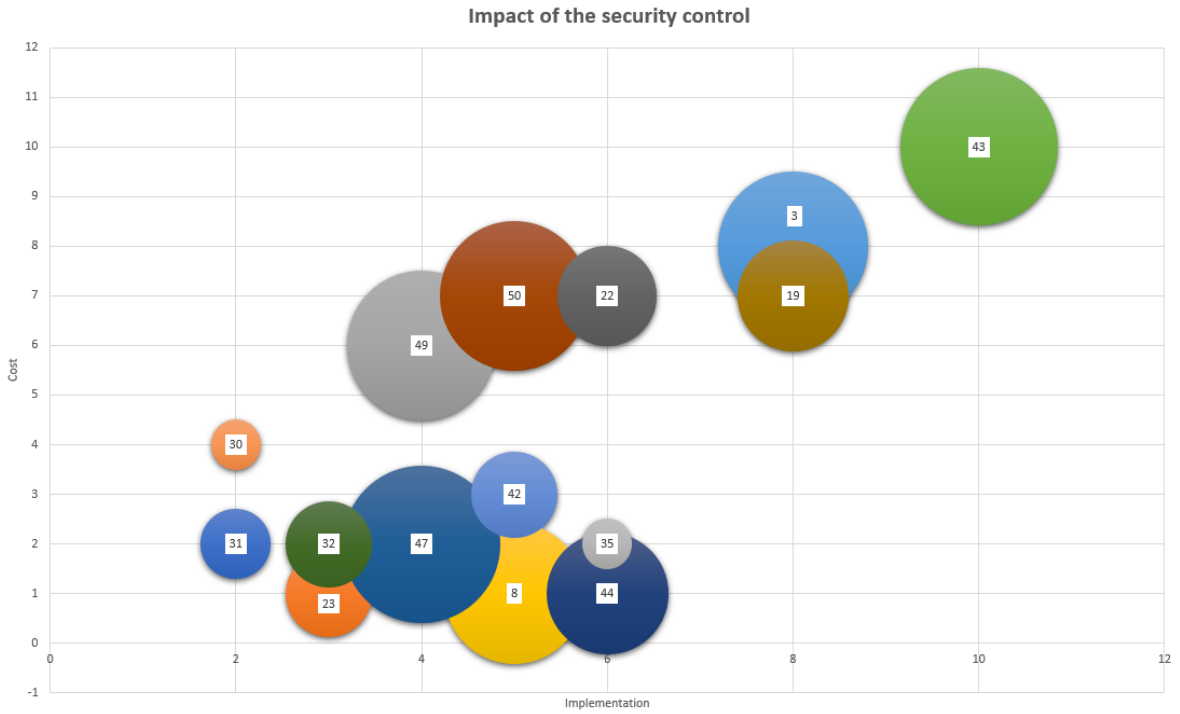
proximus NXT
cybersecurity

Thank you

antonio.paci@proximus.com

Example of intelligent management by the “security heatmap”
Cost / Complexity of implementation / Gain on security level

Risk ID	Risk
3	Vulnerability Management
8	MDM / MAM
19	Network segmentation
22	Network Access Control
23	External forwarding of corporate mail
30	split tunneling
31	Examination of suspicious files
32	3rd party supplier connections
35	VPN from internal network
42	Unmanaged systems
43	DC/DLP
44	Local Privileged Accounts
47	Strong authentication
49	Endpoint Security
50	Privileged accounts



Visual representation of the risk register anno March 2021.The visual based is upon estimations by Proximus for relative cost and relative implementation effort.
This heatmap is a living object and can change because of: new risks added to risk register, mitigated risks, cost and implementation, changes in security landscape, etc.

Example of intelligent management of security add-ons
the security risk scoremap