Analyse de la capacité de protection des hôpitaux dans le domaine informatique

Votre organisation est-elle prête à faire face à un cyberincident?

pwc

www.pwc.ch/cybersecurite

La numérisation se poursuit également dans le secteur de la santé.

Elle augmente la dépendance vis-à-vis de l'informatique.

- Ces dernières années, la numérisation et l'interconnexion du secteur de la santé se sont poursuivies.
- Le dossier électronique du patient et l'échange électronique des données des patients s'inscrivent dans cette tendance.
- Les hôpitaux doivent donc non seulement disposer de leur propre infrastructure informatique, mais également d'interfaces avec les médecins prescripteurs, les prestataires et d'autres partenaires informatiques ou commerciaux.

Les données personnelles doivent être protégées de manière «appropriée».

- Selon la loi fédérale sur la protection des données, les données médicales sont des «données sensibles».
- Les lois fédérales et cantonales exigent que les personnes qui traitent les données garantissent une «protection adéquate de ces dernières».
- Des mesures techniques et organisationnelles appropriées ainsi qu'une évaluation réaliste des risques sont dès lors requises.

Secteur de la santé

Les données électroniques contribuent à améliorer la qualité du service dans les hôpitaux, à réduire les coûts et à soigner les patients plus efficacement. Elles doivent être utilisées là où elles sont nécessaires. Différents hôpitaux ont dû mener une lutte acharnée contre des logiciels malveillantsau cours de ces derniers mois. L'hôpital Lukaskrankenhaus de Neuss (Allemagne) a par exemple dû arrêter complètement son réseau à cause de ces derniers, avec les conséquences que l'on peut s'imaginer sur son fonctionnement au quotidien. Une partie importante des cinquante opérations quotidiennes planifiées a ainsi dû être repoussée. (Février 2016).

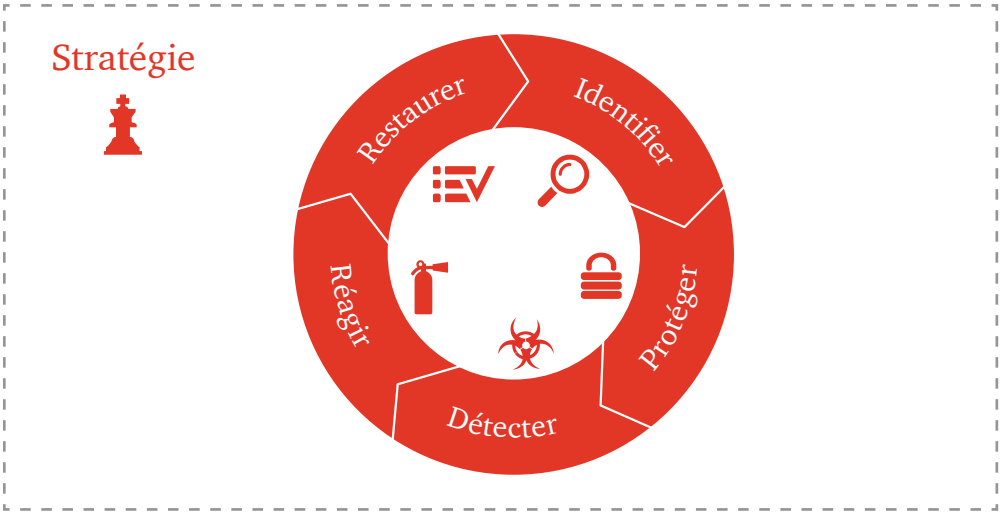
Stratégie en matière de sécurité informatique et gouvernance

- Chacun doit connaître ses données sensibles, c'est-à-dire savoir les identifier et les classifier, afin de les protéger de manière adéquate.
- Des rôles et des responsabilités clairement définis représentent les conditions d'une protection efficace des données. Les rôles de Data Owner, CISO (Chief Information Security Officer), Information Security Officer et Compliance Officerdoivent au minimum être attribués à des personnes compétentes.
- Les mesures de sécurité techniques ne vont pas de soi. Un personnel d'exploitation qualifié et suffisant ainsi que des processus afin de pouvoir mettre en œuvre les mesures informatiques de protection (IT Security Operation) sont indispensables.
- Les exigences légales et règlementaires doiventêtre connues et respectées. L'audit règlementaire exige que l'efficacité des mesures de protection et les accès aux données soient documentés (traçabilité).

Sécurité informatique: architecture de référence pour le secteur de la santé

La question n'est plus de savoir si un hôpital va subir une cyberattaque, mais plutôt quand. À l'heure actuelle, la sécurité informatique ne comporte pas uniquement des mesures de protection, mais également des possibilités de détection et de réaction face aux cyberattaques. Les technologies, les processus et les ressources humaines appropriés sont donc nécessaires.

Processus, compétences, ressources



Stratégie
Conception, gestion et surveillance de l'organisation. Gérer les risques de l'entreprise et garantir que les lois concernant le traitement des données électroniques sont respectées.

Identifier
Comprendre les ressources informatiques, les données, les processus, les interfaces ainsi que les flux de données internes ou externes et en établir l'inventaire.

Protéger
Prendre des mesures afin de protéger les données et les informations confidentielles contre les cybermenaces et les cyberattaques. Limiter l'étendue des dommages dans le cas d'une compromission.

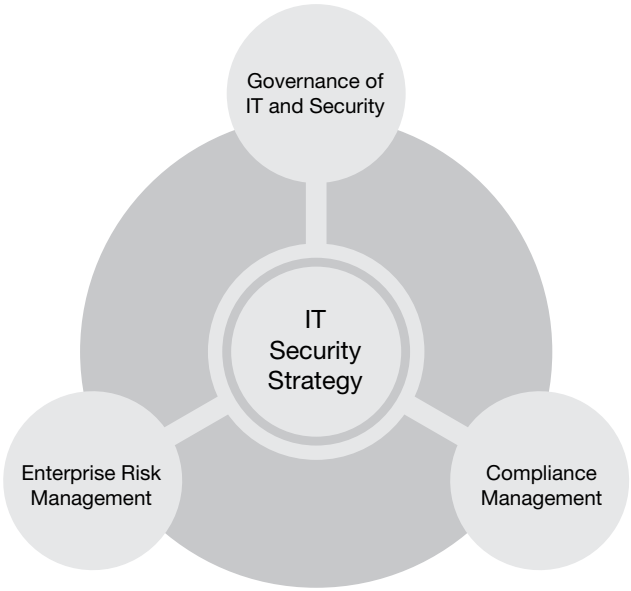
Détecter
Détecter les incidents en matière de sécurité, les attaques et les pertes de données. Prendre les mesures qui s'imposent. Impliquer les ressources d'informations sur les menaces régionales et du secteur.

Réagir
Délimiter, coordonner et classer les mesures. Procéder à l'escalade auprès de la gestion des crises en cas de nécessité.

Restaurer
Maîtriser les incidents en matière de sécurité, restaurer l'état de fonctionnement normal et minimiser les conséquences pour l'hôpital.

Gouvernance et leadership

Quels facteurs influencent la stratégie de votre entreprise sur les trois à cinq années à venir et quelles sont leurs conséquences sur la sécurité informatique? Connaissez-vous les risques encourus par votre organisation? Comment celle-ci les gère-t-elle? Quelles sont les menaces qui pèsent sur votre organisation à l'heure actuelle et dans un avenir proche?



Gouvernement de l'entreprise: gouvernance informatique / en matière de sécurité

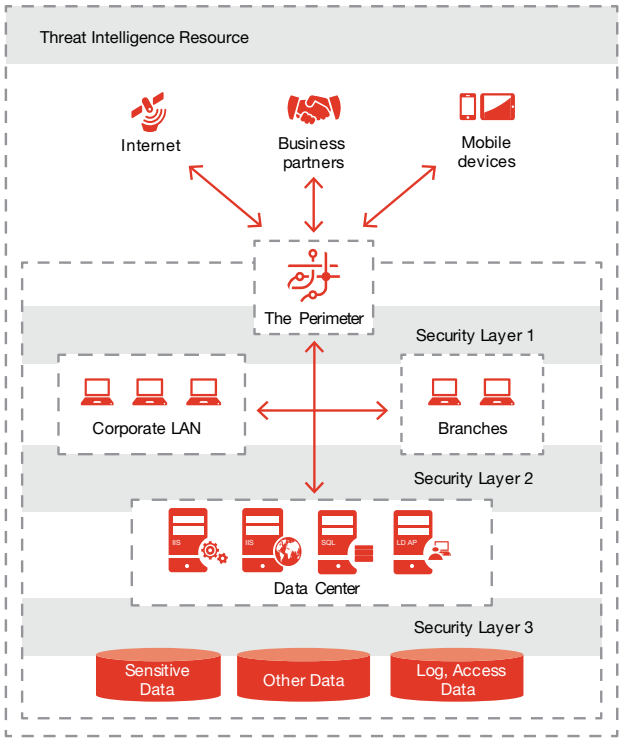
Elle comporte tous les principes de gestion et de surveillance d'une entreprise. L'informatique et les processus métier sont étroitement liés. Le conseil d'administration définit les objectifs, les procédures, les rôles et les responsabilités que la direction communique et supervise.

Gestion des risques au sein de l'entreprise: cyber-risques

La gestion des risques au sein de l'entreprise (ou ERM, Enterprise Risk Management) est une approche globale qui comporte les différentes perspectives, comme les cyber-risques, les risques opérationnels ou technologiques, les risques en matière de marché et de monnaie.

Gestion de la conformité

La gestion de la conformité comporte toutes les mesures qui permettent de garantir cette dernière. L'objectif de la gestion de la conformité consiste à garantir le respect des lois et des directives de l'entreprise ou du groupe, ainsi que la traçabilité en vue des contrôles.



Protection du périmètre

Il faut tout particulièrement surveiller les accès à partir de l'extérieur et les transferts de données vers l'extérieur (accès par des partenaires, e-mails, accès à distance, WLAN pour les visiteurs).

Transparence des tous les appareils informatiques sur le réseau

Tous les appareils informatiques raccordés au réseau de l'entreprise doivent faire l'objet d'un inventaire. Leur configuration et la version de leurs logiciels doivent être vérifiées et mis à jour, le cas échéant.

Supervision en vue de la traçabilité

Afin de pouvoir identifier les attaques de manière précoce, les données d'accès, du réseau et des fichiers journaux des systèmes ainsi que le trafic sur le réseau doivent être analysés en permanence.

Protection des accès aux données sensibles

Les données personnelles doivent uniquement être enregistrées et traitées sur des systèmes qui disposent de mesures de sécurité adéquates. Seuls les appareils conformes aux règles de sécurité d'utilisateurs identifiés sont autorisés à accéder aux données dont ces derniers ont besoin ou qu'ils doivent connaître dans le cadre de leurs activités.

Les prestations que PwC peut vous proposer: analyse des possibilités de protection dans le secteur informatique au sein de l'hôpital

Phase 1	Phase 2				Phase 3
Planification	Analyse et benchmarking des compétences, des processus et des ressources				Rapport et communication
	Preuves	1: identifier	2: vérifier	3: planifier	
Définir l'objectif et le périmètre Définir les acteurs clés	Entretien Analyse des documents	Comprendre les processus et les work-flows	Vérifierl' efficacité des mesures de sécurité	Établir la priorité des étapes suiv-antes en vue d'améliorer la cyber-sécurité	Établir un rapport et discuter avec les parties prenantes
Identifier les documents à analyser	Analyse des processus	Interroger les acteurs clés Suivre les données, les processus et les systèmes à partir de 2–3 workflows	Identifier les failles et les améliorations possibles Effectuer un benchmark par rapport aux bonnes pratiques du secteur		Faire une présenta-tion à l'attention de la direction et du conseil d'administration (si vous le souhaitez)

PWC a conçu une méthode d'analyse spécifique au secteur de la santé afin de fournir à la direction et au conseil d'administration des hôpitaux des informations claires sur le respect des exigences concernant la protection des données et sur la capacité de leur organisation à détecter les cyberincidents, à les évaluer ainsi qu'à les gérer de manière efficace.

Phase	Activité	Livrables
1	• Réunion de lancement avec les acteurs clés • Délimitation du périmètre et planification détaillée	Plan détaillé de l'évaluation
2	• Identifier les règles et les normes • Sélectionner entre 3 et 5 processus métiers dans lesquels des données confidentielles sont traitées • Recenser les flux de données, les systèmes et les mesures de sécurité • Vérifier si les données sont protégées selon les directives et les normes du secteur • Analyser les écarts entre la référence de PwC et la situation actuelle en ce qui concerne les compétences, les ressources, les processus et la technologie	Benchmark concernant les personnes, les processus et la technologie Analyse des écarts: • directives applicables • normes du secteur
3	• Rapports et présentation • Établir la priorité des mesures	• Présentation • Rapport

Étapes nécessaires en vue de l'amélioration permanente

1. Concevoir et mettre en œuvre une stratégie dans le domaine de l'informatique et de la sécurité. Mettre en place la gouvernance dans le domaine de l'informatique et de la sécurité en identifiant les ressources informatiques sensibles (données, systèmes informatiques, processus), établir et mettre à jour un inventaire.
2. Sélectionner les scénarios vraisemblables des menaces et analyser les conséquences des incidents en matière de sécurité sur l'organisation en ce qui concerne la confidentialité, la disponibilité et l'intégrité des données ainsi que les systèmes informatiques.
3. Vérifier l'efficacité des mesures de sécurité mises en œuvre (sur le plan technique et organisationnel) et identifier les points faibles.
4. Évaluer et documenter les risques dans les domaines de la sécurité et de la technologie pour chaque application métier, les gérer en permanence. Cette étape comprend l'évaluation des risques et leur gestion.
5. Superviser en permanence les mesures de protection et les données au moyen d'un personnel qualifié. Détecter et gérer efficacement les incidents en matière de sécurité. Tirer sans cesse les leçons des incidents en matière de sécurité et identifier les nouvelles menaces.

Modules supplémentaires en option:

«Game of Threat»: simulation de cyberattaques à l'attention de la direction	Penetration Tests: (i) à partir de l'extérieur (ii) à partir de l'intérieur, (iii) ingénierie sociale	Compromise Discovery Assessment: évaluation de la détection des compromissions en faisant appel aux informations sur les menaces	Conseil juridique et évaluation de la préparation en ce qui concerne la protection des données et le Règlement général sur la protection des données de l'Union Européenne	Cloud Readiness Assessment: évaluation du niveau de préparation de votre organisation afin d'adopter le cloud

www.pwc.ch/cybersecurite

Reto Häni
Partner and Leader Cybersecurity
PwC Digital Services, Switzerland
+41 58 792 75 12
reto.haeni@ch.pwc.com

Jean Paul Ballerini
Director Cybersecurity
PwC Digital Services, Switzerland
+41 58 792 26 97
jean.paul.ballerini@ch.pwc.com

Urs Küderli
Director Cybersecurity Strategy and Transformation
PwC Digital Services, Switzerland
+41 58 792 42 21
urs.kuederli@ch.pwc.com

Lorenz Neher
Senior Manager Cybersecurity Security Technology
PwC Digital Services, Switzerland
+41 58 792 47 85
lorenz.neher@ch.pwc.com

www.pwc.ch/secteur-sante

David Roman
Director
PwC Switzerland
+41 58 792 77 90
david.roman@ch.pwc.com