

ÉTUDE DES TENDANCES

SERVICES DE SÉCURITÉ GÉRÉS EN SUISSE:

Aperçu de l'évolution et de la structure du
marché

Lead Analyst:

Wolfgang Schwab

teknowlogy Group, janvier 2020

En coopération technique avec



TABLE DES MATIÈRES

INTRODUCTION	3
ÉVOLUTIONS DU MODÈLE DE SÉCURITÉ INFORMATIQUE.....	3
SÉCURITÉ INFORMATIQUE ET CLOUD COMPUTING	4
SERVICES DE SÉCURITÉ GÉRÉS	5
MOTIVATION DU POINT DE VUE DE L'UTILISATEUR	6
ÉVOLUTION DU MARCHÉ	7
TENDANCES ET MOTEURS DE LA CYBERSÉCURITÉ EN EUROPE ET EN SUISSE	7
MARCHÉ ET CROISSANCE DES SERVICES DE SÉCURITÉ GÉRÉS EN SUISSE	8
IMPORTANCE POUR LES UTILISATEURS INDIVIDUELS	10
STRUCTURE DU MARCHÉ	11
CATÉGORISATION DES FOURNISSEURS DE SERVICES.....	11
QUELS SONT LES FOURNISSEURS ADAPTÉS POUR CHAQUE CLIENT?	12
RÉSUMÉ ET RECOMMANDATIONS	14
ANNEXE	16
AVIS DE NON-RESPONSABILITE, DROITS D'UTILISATION, INDEPENDANCE ET PROTECTION DES DONNEES	16
À PROPOS DE SWISSCOM BUSINESS CUSTOMERS	18
À PROPOS DE TEKNOLOGY GROUP	19

INTRODUCTION

S'il est un sujet qui anime le secteur des technologies de l'information, mais aussi l'économie dans son ensemble depuis des années, c'est bien la sécurité des systèmes informatiques sous toutes leurs formes.

ÉVOLUTIONS DU MODÈLE DE SÉCURITÉ INFORMATIQUE

Le modèle des dernières décennies, à savoir la focalisation sur la sécurité périmétrique, a toujours été controversé, car l'isolement des « bons » systèmes internes par rapport au monde extérieur « néfaste » ne fonctionne pas. À l'avenir, il pourrait d'ailleurs de moins en moins fonctionner, car les frontières entre les systèmes internes et externes s'estompent.

D'une part, les appareils mobiles, le cloud computing et l'économie numérique impliquent une multiplication des points d'accès aux ressources internes qui doivent être sécurisés. C'est particulièrement vrai pour les terminaux, dont le nombre a rapidement augmenté et qui sont équipés de plus en plus d'applications. Par ailleurs, les services informatiques n'ont pas le contrôle total sur une grande partie de ces appareils, qui sont également utilisés à des fins privées. Le contrôle et la sensibilisation des utilisateurs revêtent ici une grande importance.

Tous ces constats montrent que l'ère de la « forteresse » classique, qui reposait principalement sur la sécurité périmétrique, est bel et bien révolue.



Fig. 1 : De la forteresse à l'aéroport

De nos jours, une stratégie de sécurité nécessite une approche différente, semblable à celle d'un aéroport moderne. Il devrait y avoir différentes zones de sécurité, ouvertes ou fortement sécurisées selon les besoins, et suffisamment flexibles et intelligentes pour identifier les menaces futures en analysant les différents comportements des utilisateurs internes ou externes en contexte ou les différents schémas de flux d'informations. Par conséquent, l'intelligence artificielle (IA), l'apprentissage automatique et l'analytique Big Data sont devenus indispensables pour de nombreuses solutions de sécurité. Les principaux avantages de la cybersécurité

basée sur l'IA ? La possibilité de surveiller intégralement le trafic et les actions des utilisateurs et, dans une certaine mesure, l'automatisation des réponses complexes.

Les technologies encore émergentes et les risques associés à l'approche « boîte noire » de l'apprentissage automatique, ainsi que la subtile possibilité d'attaque par « empoisonnement du puits », c'est-à-dire la manipulation de l'ensemble de données de formation, constituent les principaux défis actuels. Pour de nombreux services informatiques, la technologie entourant l'IA est actuellement trop immature et trop complexe à mettre en œuvre. Cela ne signifie pas que les solutions de sécurité classiques, telles que la sécurité des terminaux, sont obsolètes. Elles doivent cependant être améliorées dans le cadre d'une architecture de sécurité globale afin d'être prêtes à faire face au nombre croissant de menaces informatiques et de cybersécurité, et notamment aux scénarios susceptibles d'évoluer à l'avenir.

Par conséquent, les DSI et les responsables de la sécurité doivent définir et mettre en œuvre une stratégie et une architecture de sécurité globales.

SÉCURITÉ INFORMATIQUE ET CLOUD COMPUTING

Dans les nouvelles entreprises numériques, le cloud computing constitue la norme *de facto* et représente une part toujours plus importante de l'environnement informatique pour une grande majorité des entreprises et administrations. À ses débuts, le cloud était principalement limité à certains services SaaS publics, mais l'IaaS et le PaaS ont évolué rapidement et sont maintenant fortement représentés dans de nombreuses entreprises. La plupart des entreprises disposent de systèmes informatiques hybrides très hétérogènes. Ceux-ci comprennent différents types de services cloud hérités, privés, publics, locaux et hébergés, et sont très souvent répartis entre différents fournisseurs et technologies.

Cette complexité est le principal ennemi de la cybersécurité, et ce tableau complexe laisse clairement transparaître que la surface d'attaque est gigantesque, qu'il est difficile de la contrôler et que les failles de sécurité peuvent être nombreuses. Les services informatiques réalisent généralement rapidement qu'il leur est impossible, ou du moins très difficile, de gérer cette complexité en interne.

SERVICES DE SÉCURITÉ GÉRÉS

Pour diverses raisons que nous verrons plus loin, il est logique que les entreprises utilisent des services de sécurité gérés, et elles le font de plus en plus. Le facteur décisif étant que le fournisseur de services peut garantir le service géré en tant que tel, mais aussi proposer un support de projet et en amont en termes de stratégie et d'architecture. Les centres des opérations de sécurité (Security Operations Centers, SOC) et les équipes de réponse aux incidents de sécurité informatique (Computer Security Incident Response Teams, CSIRT) devraient faire partie de l'offre de services, au même titre que l'exploitation d'infrastructures de sécurité informatique dans le domaine de la prévention. C'est la seule façon de garantir une cybersécurité globale et de l'améliorer en permanence.



MOTIVATION DU POINT DE VUE DE L'UTILISATEUR

La digitalisation représente un défi important pour les entreprises: d'une part, les modèles commerciaux existants doivent être optimisés et, d'autre part, de nouveaux modèles commerciaux doivent être trouvés sans compliquer indûment le cœur de métier. L'expérience client est tout aussi importante que la communication optimale entre les clients et les fournisseurs pour pouvoir mettre en œuvre les concepts de base de la digitalisation. En outre, de nouveaux modèles de déploiement tels que le cloud computing ont révolutionné le développement de logiciels et continueront de le faire. Les exigences que les services informatiques doivent remplir en matière d'agilité et de compétence méthodologique augmentent ainsi drastiquement. Parallèlement, il faut bien sûr garantir la conformité et la sécurité informatique, une tâche toujours plus complexe en raison de l'augmentation des menaces et des exigences de conformité plus strictes et qui, pour de nombreuses raisons, ne peut être facilement assurée en interne.

C'est pourquoi les entreprises recherchent le soutien de fournisseurs de services informatiques afin de se libérer des tâches de routine quotidiennes, d'une part, et de pouvoir s'appuyer sur les bonnes pratiques et les modèles d'approche pour des projets stratégiques, d'autre part. Par conséquent, le marché des services de sécurité connaît une évolution extrêmement positive dans l'ensemble. La question reste bien sûr de déterminer le fournisseur de services qui convient le mieux à chaque entreprise. Pour y répondre, des aspects tels que l'étendue et la



« Swisscom est elle-même une entreprise qui fournit et exploite des infrastructures stratégiques. Rien que pour cette raison, nous avons une grande expérience en cybersécurité et la partageons avec nos clients. »

**Lorenz Inglin,
Head of Cyber Defense, Swisscom**

profondeur du portefeuille de solutions sont tout aussi importants que la présence régionale du client et du fournisseur de services. Il importe ici de déterminer avec précision les attentes envers le fournisseur de services qui peuvent être satisfaites dans chaque cas particulier.

ÉVOLUTION DU MARCHÉ

La demande en services de cybersécurité augmente à un rythme supérieur à la moyenne en Suisse. Cette croissance est alimentée par les tendances décrites ci-dessous.

TENDANCES ET MOTEURS DE LA CYBERSÉCURITÉ EN EUROPE ET EN SUISSE

Les tendances et moteurs les plus importants de la cybersécurité peuvent être présentés comme suit:

- La cybercriminalité continue d'augmenter tant en quantité qu'en complexité, ce qui se traduit par une plus grande prise de conscience du problème. C'est vrai en Suisse comme en Europe, mais aussi dans le reste du monde.
- La cybersécurité est devenue une question stratégique qui doit être abordée au niveau de la direction et recevra certainement toute l'attention nécessaire. Cela s'applique à la fois à l'Europe et à la Suisse, à l'instar de l'écart d'attention entre les grandes entreprises et les petites.
- La conformité au règlement général sur la protection des données (RGPD), à la directive sur la sécurité des réseaux et des systèmes informatiques (NIS) et aux nombreuses réglementations sectorielles (en particulier dans le domaine des infrastructures stratégiques ou des services financiers) qui imposent des jalons à court terme augmente à la fois la charge de travail et la responsabilité des employés chargés des données internes et de la conformité. Le RGPD et la directive NIS sont certes tous deux pilotés par la Communauté européenne, mais le RGPD s'applique au monde entier dès lors qu'il est question de données personnelles des citoyens de l'Union européenne (UE). Cela signifie que lorsque des entreprises suisses traitent des données personnelles de citoyens de l'UE, elles sont soumises au RGPD. La directive NIS concerne également les entreprises suisses qui possèdent des succursales dans d'autres pays de l'UE.
- Avec l'adoption croissante du cloud, la pression pour mettre en œuvre une stratégie de sécurité complète de l'infrastructure



« De nombreuses entreprises suisses ont encore du respect pour le cloud computing et l'utilisent de manière très pesée, c'est-à-dire sous une forme hybride qui combine l'exploitation classique de centres de données et le cloud privé/public. Dans ce contexte, la cybersécurité joue un rôle majeur. »

**Cyrill Peter,
Head of Enterprise Security, Swisscom**

informatique augmente. Le « shadow IT », c'est-à-dire l'acquisition et l'exploitation non coordonnées de solutions informatiques dans des services spécialisés, crée des vulnérabilités qui ne relèvent pas du champ d'action normal du service en charge de la sécurité informatique, mais présentent un potentiel de risque massif.

- La transformation digitale actuellement amorcée dans de nombreuses entreprises augmente le volume de données à risque, qui englobent même l'identité des clients. L'introduction de méthodes Agile et de DevOps nécessite un nouveau modèle de sécurité. C'est vrai en Suisse comme en Europe. En Amérique du Nord, les entreprises ont une certaine longueur d'avance, de sorte que les bonnes pratiques locales peuvent être adaptées et reprises.
- Une importante pénurie d'experts en sécurité informatique entraîne une demande croissante en services de sécurité gérés et professionnels.

MARCHÉ ET CROISSANCE DES SERVICES DE SÉCURITÉ GÉRÉS EN SUISSE

Le marché des logiciels de sécurité devrait atteindre 555 millions de francs suisses en 2020, soit une croissance de 8,9% par rapport à 2019. À titre de comparaison, le marché des services de sécurité représente 839 millions de francs suisses en 2020, soit une croissance de 11,2% par rapport à 2019. En conséquence, on peut affirmer que l'intérêt pour les services de sécurité augmente considérablement.

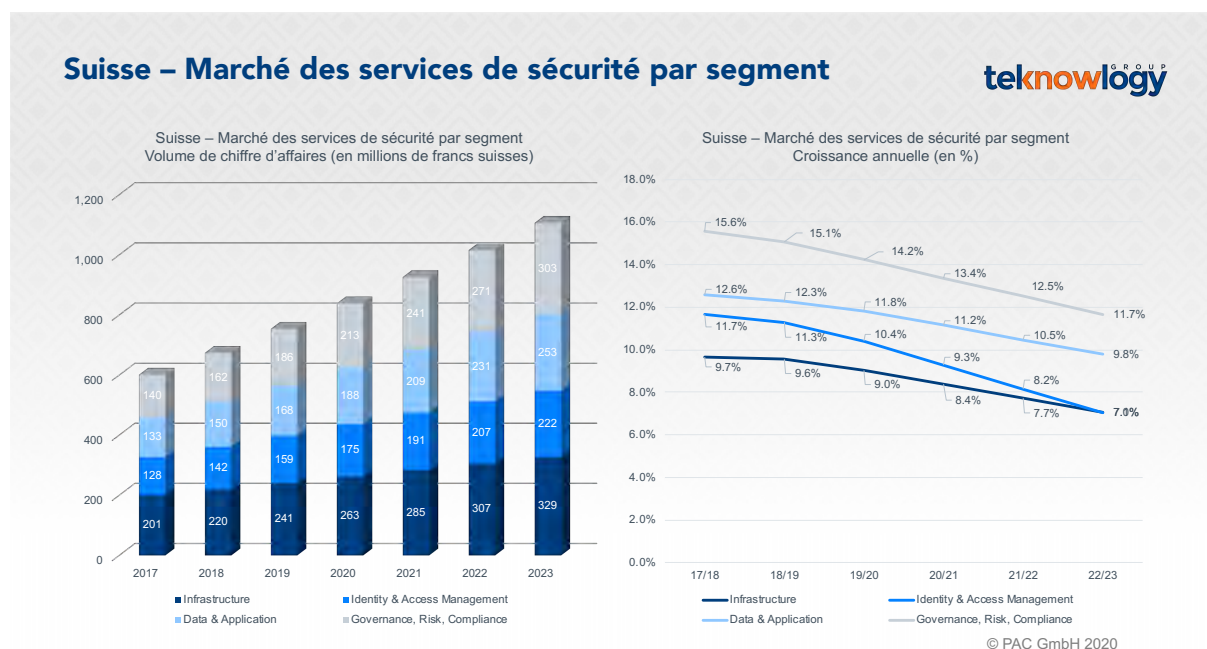


Fig. 2 : Suisse – Marché des services de sécurité par segment

Si l'on examine plus en détail les services de sécurité, on constate qu'une grande partie des services de sécurité touchent au domaine du conseil et de l'intégration

de systèmes, et que l'externalisation (en particulier les services de sécurité gérés) est encore capable d'évoluer. C'est principalement dû aux grandes entreprises et aux banques, qui dépendent encore souvent de leurs propres opérations mais recherchent un soutien pour des projets de conseil et d'intégration de systèmes. Les petites et moyennes entreprises, en revanche, sont nettement plus ouvertes à l'idée d'un service géré, notamment parce qu'elles n'ont pratiquement pas de personnel qualifié en interne capable d'assurer le fonctionnement de plus en plus complexe.

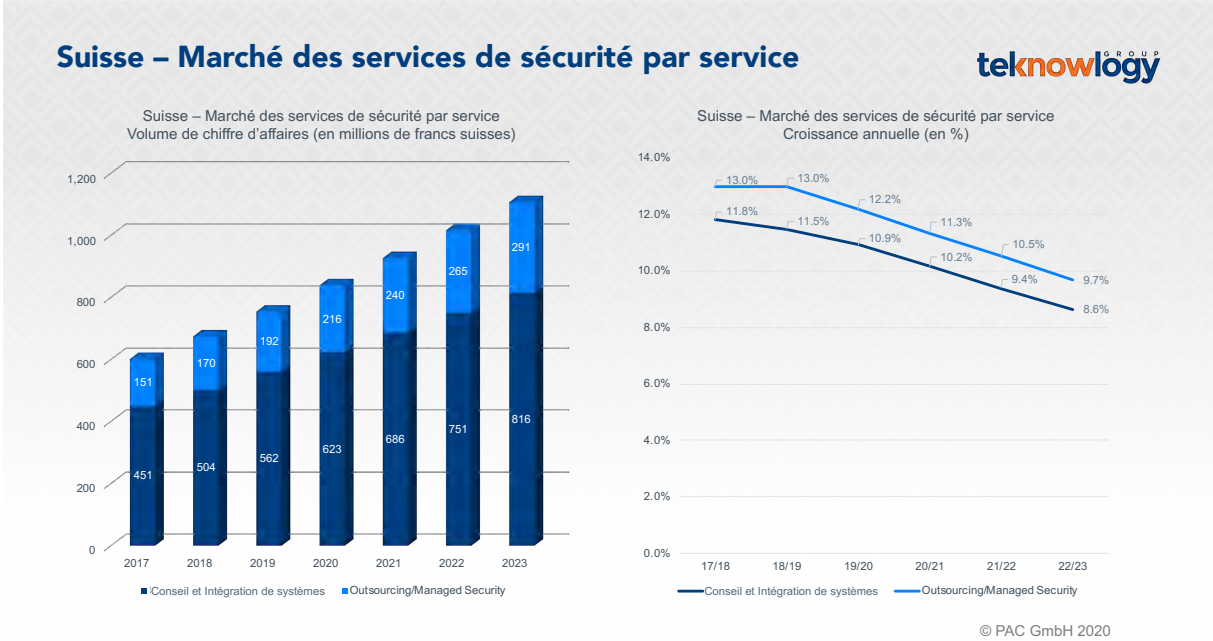


Fig. 3 : Suisse – Marché des services de sécurité par service

IMPORTANCE POUR LES UTILISATEURS INDIVIDUELS

Les utilisateurs doivent s'adapter aux tendances et aux défis. Toutes les entreprises ne sont pas touchées dans la même mesure par toutes ces évolutions, mais elles devraient toujours en tenir compte dans leurs réflexions stratégiques et tactiques et se demander notamment si les stratégies, les architectures, mais aussi les modalités de projet et de fonctionnement actuelles seront encore viables à l'avenir, ou s'il ne faudrait pas recourir à des services de sécurité gérés dès que possible. À l'heure de la digitalisation, les utilisateurs peuvent de moins en moins se permettre de tolérer des faiblesses en matière de sécurité informatique. La pénurie de spécialistes, d'une part, et la menace de sanctions, d'autre part, ainsi que l'atteinte à la réputation en cas d'attaques réussies, nécessitent une architecture de sécurité informatique qui fonctionne de façon optimale.



« Les services de sécurité gérés présentent un grand avantage: la courbe d'apprentissage et l'évolutivité reposent sur un grand nombre d'entreprises. Cela permet une meilleure protection à moindre coût. »

**Cyrill Peter,
Head of Enterprise Security, Swisscom**

STRUCTURE DU MARCHÉ

Comme en Europe et dans le monde, le marché des services de sécurité informatique en Suisse est encore très fragmenté, c'est-à-dire qu'on n'observe pas (comme c'est habituellement le cas sur les marchés matures) un nombre réduit de très grands fournisseurs et une série de spécialistes plus petits. Cela peut s'expliquer par la forte dynamique de l'environnement de sécurité sous l'effet des nouvelles technologies de prévention des risques (l'IA, par exemple), des nouvelles menaces (les pirates professionnels, par exemple) et des nouveaux vecteurs de menace (l'IloT ou Internet industriel des objets, ou encore l'intégration IT-OT ou intégration des technologies de l'information commerciales et du traitement des données liées à la production).

CATÉGORISATION DES FOURNISSEURS DE SERVICES

Il est possible de regrouper les fournisseurs de services de sécurité informatique sur la base de deux vecteurs: d'une part, l'orientation géographique (concentration suisse ou prestataires internationaux) et d'autre part, l'effort requis pour la gestion des fournisseurs. Les fournisseurs de services ou les magasins spécialisés dans la sécurité informatique proposent certes un bon service, mais impliquent davantage de travail, car il faut envisager d'autres interlocuteurs et gérer plus de contrats de service. Des efforts supplémentaires que la plupart des services informatiques ou des organisations des responsables de la sécurité informatique (Chief Information Security Officer, CISO) déjà surchargés peuvent difficilement se permettre et ne sont pas prêts à faire. La troisième catégorie comprend les fournisseurs suisses et internationaux qui proposent des solutions de sécurité informatique sous forme de logiciels, mais qui dispensent également des services de conseil, d'intégration de systèmes et de gestion dans le cadre de leurs portefeuilles de solutions souvent spécifiques.

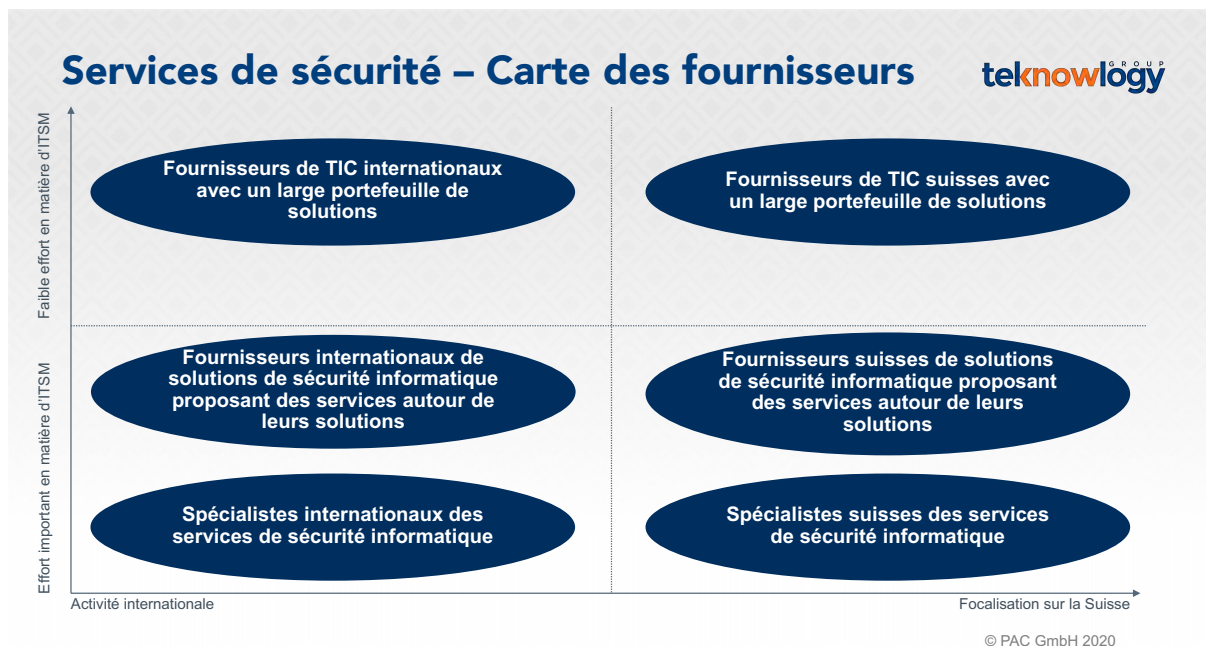


Fig. 4 : Services de sécurité informatique gérés – Carte des fournisseurs

Les mêmes défis se posent que pour les fournisseurs de services ou les magasins spécialisés dans la sécurité informatique, bien que dans ce cas, le nombre de contrats de service potentiels augmente encore plus.

QUELS SONT LES FOURNISSEURS ADAPTÉS POUR CHAQUE CLIENT?

Tous les fournisseurs ne conviennent pas à tous les clients et vice versa. On peut identifier trois groupes d'utilisateurs affichant des besoins très différents:

- Les petites et moyennes entreprises (PME):** pour la plupart à vocation nationale, ces entreprises ont relativement peu d'expérience dans la gestion des fournisseurs de services informatiques. Par conséquent, un partenaire qui couvre non seulement certains aspects de la sécurité mais aussi les technologies de l'information dans leur ensemble est généralement plus approprié. La proximité locale est également souhaitée par ce groupe de clients, ce que les petits fournisseurs de services informatiques et les multinationales ne peuvent souvent pas offrir. Par conséquent, les fournisseurs de services informatiques disposant d'un large portefeuille de technologies et de bureaux locaux sont idéaux pour les PME.

- **Les grandes entreprises principalement actives en Suisse:** ces entreprises ont généralement une expérience en gestion des fournisseurs de services informatiques, mais sont dispersées à l'échelle nationale, de sorte qu'une certaine proximité locale peut être avantageuse pour elles aussi. Parallèlement, un fournisseur de services informatiques bénéficiant d'une large présence constitue un avantage, car la gestion se complexifie avec chaque fournisseur de services supplémentaire. Par conséquent, les grandes entreprises qui se concentrent clairement sur la Suisse sont également plus susceptibles de s'intéresser à des fournisseurs de services informatiques affichant un large portefeuille de solutions et une présence locale.
- **Les grandes entreprises (« multinationales suisses »):** les multinationales qui sont également actives en Suisse ou y ont leur siège doivent, d'une part, assurer les opérations informatiques mondiales et leur sécurité et, d'autre part, s'adapter aux conditions locales telles que les exigences de conformité. Elles ont généralement une grande expérience en gestion des fournisseurs de services, et certaines d'entre elles disposent d'une fonction centralisée de gestion informatique et de gouvernance. Pour les multinationales, dont la gestion informatique tend à être orientée à l'échelle nationale, il en va de même que pour les grandes entreprises principalement actives en Suisse, c'est-à-dire que les fournisseurs de services informatiques affichant un large portefeuille de solutions sont intéressants. Les multinationales qui disposent d'une fonction centralisée de gestion informatique et se concentrent sur des solutions homogènes au niveau international sont plus susceptibles de se tourner vers des fournisseurs de services informatiques affichant un large portefeuille de solutions et une présence internationale.



« Swisscom compte plus de 200 experts en cybersécurité, avec des SOC à Zurich et Genève. »

**Cyrill Peter,
Head of Enterprise Security, Swisscom**



RÉSUMÉ ET RECOMMANDATIONS



Services de sécurité informatique en Suisse

Par rapport aux autres pays européens, la part des services de sécurité informatique dans les dépenses totales pour sécurité informatique en Suisse est inférieure d'environ 7 points de pourcentage. Parallèlement, la part de l'externalisation de la sécurité informatique est supérieure d'un point de pourcentage à celle des autres pays européens. Cela signifie que les entreprises suisses préfèrent déployer elles-mêmes des solutions de sécurité et les faire ensuite exploiter par leur propre personnel.



Développer soi-même ou acheter, une décision déterminante

Posez-vous les questions suivantes : les mécanismes de sécurité existants sont-ils vraiment bien adaptés aux menaces actuelles? Comment pourrait-on les améliorer? Est-il judicieux, d'un point de vue économique, de développer ou d'élargir ses propres compétences? Ne vous contentez pas de considérer l'infrastructure et les terminaux. La sécurité des applications et des données est également décisive. Enfin, les mesures de sécurité ne sont efficaces que si elles sont combinées à une analyse « intelligente » des menaces et des vulnérabilités.



Tous les fournisseurs de services de sécurité informatique ne conviennent pas à tous les clients

Posez-vous les questions suivantes : combien de fournisseurs de services informatiques différents peuvent être gérés efficacement? Mes exigences géographiques correspondent-elles à celles du partenaire potentiel? Consultez les fournisseurs potentiels de services de sécurité informatique pour comprendre leur portefeuille de solutions de cybersécurité et déterminer si celles-ci sont compatibles avec vos investissements existants. Découvrez comment les fournisseurs de services de sécurité peuvent répondre aux exigences propres à votre secteur et à vos processus.



Fournisseurs de services complets ou spécialistes

La définition des exigences de sécurité est un processus itératif qui devrait être revu régulièrement. Il convient de déterminer clairement si l'on a besoin d'un fournisseur de services complets qui s'occupe de l'ensemble de l'environnement informatique ou d'un spécialiste qui se concentre sur certains domaines. N'oubliez pas que le multisourcing peut améliorer les capacités de détection des menaces, d'alerte et de correction, mais qu'il est aussi beaucoup plus complexe à gérer.



Le triangle « Personnes, processus et technologie » est décisif

La sécurité informatique concerne aussi bien les personnes et les processus que la technologie. Les fournisseurs de services gérés peuvent s'avérer être de précieux partenaires pour identifier et améliorer les bonnes pratiques en matière de comportement des utilisateurs finaux (bonne hygiène de sécurité, par exemple) et de processus de sécurité (réponse aux incidents, par exemple). Toutefois, le recours à des fournisseurs de services gérés n'implique aucune délégation de responsabilité: les organisations d'utilisateurs informatiques elles-mêmes restent toujours responsables en dernier ressort.



Cloud computing et sécurité ne sont pas contradictoires

Tirez pleinement parti du « cloud computing ». Grâce au cloud, les fournisseurs de services gérés peuvent proposer des services de sécurité hautement évolutifs pour faire face au nombre considérable de menaces auxquelles sont confrontées les entreprises. La mise en œuvre (ou la mise à l'échelle) de technologies coûteuses n'est plus nécessaire pour atteindre un bon niveau de sécurité.



La carte de la sécurité informatique ne peut compter de lacunes

Veillez à ce que les fournisseurs de services sélectionnés puissent fournir des services de sécurité dans tous les domaines d'intérêt, par exemple le cloud computing, l'IoT, les centres de données, l'edge computing, les réseaux, les utilisateurs finaux, etc. La cybersécurité est un problème systémique et holistique.

ANNEXE

AVIS DE NON-RESPONSABILITE, DROITS D'UTILISATION, INDEPENDANCE ET PROTECTION DES DONNEES

Cette étude a été réalisée pour le compte de Swisscom.

Pour plus d'informations, rendez-vous sur www.vendor.teknowlogy.com.

Avis de non-responsabilité

Les contenus de cette étude ont été compilés avec le plus grand soin. Toutefois, aucune garantie ne peut être donnée quant à leur exactitude. Les avis et évaluations reflètent l'état actuel des connaissances en janvier 2020 et peuvent évoluer à tout moment. Cela s'applique en particulier, mais pas exclusivement, aux déclarations prospectives. Les noms et appellations figurant dans cette étude sont susceptibles d'être des marques déposées.

Droits d'utilisation

Cette étude est protégée par le droit d'auteur. Toute reproduction ou cession à des tiers, même partielle, requiert le consentement explicite préalable de son auteur. La publication ou la diffusion de tableaux, graphiques, etc. dans d'autres publications requiert une autorisation préalable.

Indépendance et protection des données

Cette étude a été réalisée par PAC – a teknowlogy Group Company. Le client n'a eu aucune influence sur l'analyse des données et la préparation de l'étude.

LISTE DES FIGURES

Fig. 1 : De la forteresse à l'aéroport..... 3

Fig. 2 : Suisse – Marché des services de sécurité par segment..... 8

Fig. 3 : Suisse – Marché des services de sécurité par service 9

Fig. 4 : Services de sécurité informatique gérés – Carte des fournisseurs..... 12

À PROPOS DE SWISSCOM BUSINESS CUSTOMERS



La division Business Customers de Swisscom constitue le plus grand fournisseur intégré de TIC pour les entreprises et les PME en Suisse. Ses principales compétences sont les suivantes:

- Solutions de communication intégrées
- Infrastructure informatique et services cloud
- Sécurité informatique
- Solutions de poste de travail
- Services SAP
- IoT
- Services complets d'externalisation pour le secteur financier et les soins de santé

Avec environ 5 000 employés, Swisscom Business Customers répond aux besoins de plus de 6 000 clients « Grands comptes » et de plus de 300 000 PME.

La sécurité chez Swisscom Business Customers

Selon des études indépendantes, Swisscom Business Customers est le premier fournisseur de services de sécurité en Suisse. Nos experts en sécurité s'engagent quotidiennement en faveur de la sécurité informatique dans les entreprises suisses. Swisscom propose à ses clients une vaste gamme de services de sécurité gérés, dédiés et éprouvés, dont un SOC disponible 24 h/24 et 7 j/7 avec accès à des spécialistes en sécurité.

Vous trouverez de plus amples informations sur le thème de la sécurité en suivant le lien ci-dessous:

www.swisscom.ch/fr/business/entreprise/offre/security

Vous avez une question ou vous souhaitez vous entretenir avec l'un de nos experts?

Prenez sans plus attendre [contact](#) avec nos experts en sécurité.

À PROPOS DE TEKNOLOGY GROUP

teknology Group se positionne comme le premier cabinet européen indépendant d'analyse et de conseil dans le domaine des logiciels, des services informatiques et de la transformation numérique. Il réunit l'expertise de deux sociétés [CXP](#) et [PAC](#), qui travaillent ensemble et de manière complémentaire pour proposer à leurs clients une expertise à 360° des marchés dans un esprit de partenariat et de partage de vision prospective.

teknology Group est une société basée sur le contenu avec un ADN en matière de conseil. teknology Group est le partenaire privilégié des entreprises européennes utilisatrices pour définir leur stratégie informatique, gérer leurs équipes et leurs projets, et réduire les risques liés aux choix technologiques qui conduisent à une transformation réussie de leur activité.

Grâce à sa connaissance des tendances du marché et des attentes des utilisateurs informatiques, teknology Group aide les éditeurs de logiciels et les sociétés de services informatiques à mieux définir, exécuter et promouvoir leur propre stratégie, en cohérence avec les besoins du marché et en anticipation des attentes de demain.

Capitalisant sur plus de 40 ans d'expérience, teknology Group est présent dans sept pays avec un réseau de 150 experts.

Pour plus d'informations, rendez-vous sur www.teknology.com et suivez-nous sur [Twitter](#) or [LinkedIn](#).



Contact:

teknology | PAC
Holzstr. 26
80469 München (Allemagne)

+49 (0)89 23 23 68 0

info-germany@pac-online.com

www.vendor.teknology.com

www.sitsi.com



teknology^{GROUP}