Aperçu des mesures techniques et organisationnelles liées à la sécurité au sein de Proximus

1. Organisation de la sécurité chez Proximus

Le département Security Governance and Investigation, placé sous l'égide de Group Corporate Affairs, a pour tâche de veiller à la gouvernance et à la gestion de la sécurité ainsi qu'à la surveillance et aux réponses en matière de cybersécurité au sein de l'organisation.

Security Governance est responsable du cadre de sécurité de l'information de Proximus, en ce compris la définition et la gestion des politiques de sécurité de l'information ainsi que l'architecture de sécurité.

Security Management a pour tâche d'évaluer la mesure dans laquelle les différents projets au sein de la société sont alignés sur les politiques de sécurité, de soumettre ces projets à des évaluations de risque pour la sécurité de l'information, de gérer les vulnérabilités et les intrusions et de mesurer la conformité aux politiques de sécurité de l'information et d'en rendre compte.

L'entité Cyber Security Intelligence & Incident Response héberge deux équipes :

- Le Cyber Defense Center, qui est l'équipe centrale de surveillance des incidents de cybersécurité touchant l'infrastructure et les services du Groupe Proximus. Avec la capacité 24x7 que lui permet le Network Operations Center dans sa globalité, le Cyber Defense Center a pour but de détecter et contenir les attaques et les intrusions dans les plus brefs délais.
- Proximus CSIRT, qui fournit des informations et une assistance visant à réduire les risques d'incidents de cybersécurité et à réagir efficacement à de tels incidents. Cette équipe se veut un exemple international d'intelligence et d'expertise en matière de cybersécurité, dans tous les domaines concernant la réaction aux incidents. Proximus CSIRT recueille, filtre, analyse et relaie les renseignements liés aux menaces, afin de communiquer de manière proactive concernant les attaques futures menées contre le Groupe Proximus.

Un "Security Officer" de liaison a été désigné pour chacune des divisions de base de Proximus, afin d'assurer une coordination directe au sein de Security Governance and Investigation et d'assurer la conformité de la division avec le cadre de sécurité établi.

2. Cadre de politique de sécurité chez Proximus

Proximus maintient un cadre de politique de sécurité englobant des contrôles et une couverture étendus des thèmes actuels et émergents touchant à la sécurité de l'information, afin de permettre à l'organisation de répondre au rythme soutenu auquel évoluent les menaces, la technologie et les risques. Dans l'ensemble du cadre de politique de sécurité établi, Proximus veille à limiter à des niveaux raisonnables les risques liés à l'information et associés à ses services, à répondre à des menaces en évolution rapide, en ce compris les attaques sophistiquées menées dans le domaine de la cybersécurité, et à respecter à tout moment les réglementations en vigueur.

Le cadre de politique de sécurité de Proximus adhère aux meilleures pratiques de la norme de bonne pratique de sécurité de l'information de l'ISF, qui couvre l'ensemble des thèmes énoncés dans les documents ISO/IEC 27002:2013, COBIT 5 for Information Security, NIST Cybersecurity Framework (cadre de cybersécurité du NIST, institut national des normes et de la technologie aux USA), CIS Top 20 Critical Security Controls for Effective Cyber Defence (top 20, établi par le CIS, des contrôles de sécurité critique pour une cyberdéfense efficace) et le Payment Card Industry Data Security Standard (PCI DSS - norme de sécurité des données de l'industrie des cartes de paiement), afin de permettre une amélioration permanente de la sécurité de l'information au sein de l'organisation et d'aider cette dernière à faire face à des incidents majeurs susceptibles d'avoir un impact significatif sur l'activité de Proximus et à gérer ces incidents.

Le cadre de politique de sécurité de Proximus est dans la lignée de la structure et du flux de la "suite" de normes ISO/IEC 27000 et permet l'adoption de multiples programmes de certification ISO 27001 au sein de l'organisation, via la mise en œuvre de systèmes de gestion de la sécurité de l'information (ISMS).

Le cadre de politique de la sécurité de Proximus traite notamment de thèmes liés aux domaines suivants :
ressources humaines, gestion des actifs, contrôle d'accès, cryptographie, sécurité physique et environnementale, sécurité d'exploitation, sécurité des communications, développement et maintenance de systèmes, relations avec les fournisseurs, gestion des incidents liés à la sécurité de l'information, gestion de la continuité des activités et conformité.

3. Gestion des risques liés à la sécurité chez Proximus

Le processus d'évaluation des risques liés à la sécurité constitue un élément de base pour garantir la sécurité et la confidentialité des données chez Proximus.

Ce processus garantit, pour tous les projets et systèmes, la mise en œuvre de contrôles de sécurité effectués par Proximus et d'une approbation accordée par des experts en sécurité avant toute mise en service.

La méthodologie d'évaluation des risques chez Proximus est alignée sur la méthodologie IRAM2 d'ISF. IRAM2 est la méthodologie standard d'entreprise applicable à tous les projets de sécurité de l'information à l'échelle de l'ensemble de Proximus et cette dernière a appliqué les systèmes de gestion de la sécurité de l'information en se basant sur ISO27001. IRAM2 est aligné sur la norme de bonne pratique de l'ISF en matière de sécurité de l'information.

4. Ressources humaines

Les contrôles de sécurité des ressources humaines poursuivent les objectifs suivants :

- veiller à ce que le personnel et les entrepreneurs comprennent leurs responsabilités et soient aptes à remplir les rôles qui leur sont confiés ;
- veiller à ce que le personnel et les entrepreneurs soient conscients de leurs responsabilités en matière de sécurité de l'information ;
- protéger les intérêts de l'organisation dans le cadre du processus de changement ou de fin d'emploi.

5. Gestion des actifs

La gestion des actifs et la classification des données chez Proximus sont instaurées pour permettre leur traçabilité et pouvoir les soumettre à un audit.

Les contrôles de sécurité de la gestion des actifs sont les suivants :

- identifier les actifs de l'organisation et définir des responsabilités adéquates en termes de protection ;
- veiller à ce que l'information bénéficie d'un niveau de protection approprié, conforme à son importance pour l'organisation ;
- empêcher toute divulgation, modification, suppression ou destruction non autorisée d'informations stockées sur des supports.

6. Contrôle d'accès

Proximus a établi différentes méthodes pour restreindre l'accès aux applications, systèmes, ordinateurs et réseaux d'entreprise en imposant aux utilisateurs de disposer

d'une autorisation avant de se voir accorder des droits d'accès, authentifiés à l'aide de mécanismes de contrôle d'accès et soumis à un processus d'approbation rigoureux.

Proximus a créé des plateformes d'identification et d'accès spécifiques pour ses clients, partenaires et collaborateurs, afin d'assurer une séparation des tâches, ainsi qu'une infrastructure spécifique de gestion d'accès privilégié.

Les contrôles de sécurité d'accès poursuivent les objectifs suivants :

- limiter l'accès à l'information et aux systèmes de traitement de l'information ;
- assurer un accès autorisé à l'utilisateur pour empêcher tout accès non autorisé aux systèmes et services ;
- rendre les utilisateurs responsables de la préservation de leurs informations d'authentification ;
- empêcher tout accès non autorisé aux systèmes et applications.

7. Cryptographie

Le cryptage permet d'augmenter encore le niveau de sécurité et de confidentialité de nos services.

Lorsque les données créées par vos soins circulent entre votre appareil, les services de Proximus et nos datacenters, elles sont protégées par une technologie de sécurité telle HTTPS et le protocole Transport Layer Security.

Chaque fois que c'est nécessaire, Proximus crypte les données personnelles hautement confidentielles et sensibles.

Les règles de sécurité de Proximus incluent aussi l'utilisation de la pseudonymisation (en remplaçant des éléments personnellement identifiables par des identifiants artificiels) et l'encodage (codage de messages, afin que seules les personnes autorisées puissent lire ces derniers).

Les contrôles cryptographiques ont pour objectif d'assurer une utilisation correcte et efficace de la cryptographie pour protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

8. Sécurité physique et environnementale

Les contrôles de sécurité physique et environnementale poursuivent les objectifs suivants :

- empêcher tout accès physique, dommage et interférence non autorisé aux informations et aux systèmes de traitement des informations de l'organisation ;
- empêcher tout vol, toute perte ou détérioration d'actifs et interruption du fonctionnement de l'organisation.

9. Sécurité des opérations

Les contrôles de sécurité des opérations poursuivent les objectifs suivants :

- assurer un fonctionnement correct et sécurisé des systèmes de traitement de l'information ;
- assurer la protection de l'information et des systèmes de traitement de l'information contre les logiciels malveillants ;
- protéger contre la perte de données ;
- enregistrer les événements et générer des éléments de preuve ;
- assurer l'intégrité des systèmes d'exploitation ;
- prévenir l'exploitation de vulnérabilités techniques ;
- minimiser l'impact des activités d'audit sur les systèmes d'exploitation.

Concernant plus spécifiquement l'exploitation des vulnérabilités techniques, Proximus a établi une procédure de gestion des vulnérabilités pour compléter le cycle de sécurité impliquant le cycle de vie des projets (contrôles préventifs) et la gestion de la réaction aux incidents (contrôles de détection) via une combinaison d'outils disponibles dans le commerce et d'outils personnalisés créés en interne, de tests de pénétration intensifs automatisés et manuels, de processus d'assurance de la qualité, d'examens de sécurité logicielle et d'audits externes.

Le processus de gestion de vulnérabilité de Proximus identifie et classe les vulnérabilités et coordonne les actions de remédiation et d'atténuation liées aux vulnérabilités susceptibles de résulter
(1) d'erreurs de conception ;
(2) d'erreurs de codage ou de code malveillant ou
(3) d'erreurs de configuration
et affectant différents éléments tels
(a) des composants de systèmes d'exploitation ou composants réseau ;
(b) des composants intermédiaires (interprètes, JRE,...) ou
(c) des "daemons", applications, firmwares, etc.

Lorsque les vulnérabilités sont identifiées, un chemin correctif est emprunté, impliquant des changements au niveau du réseau, l'installation de patches de sécurité, la correction

d'erreurs de configuration ou encore la correction de codes ou de conceptions d'applications. Proximus peut ainsi détecter les menaces et y parer pour protéger les produits contre les spams, les logiciels malveillants, les virus et les autres formes de code malveillant.

10. Sécurité des communications

Les contrôles de la sécurité des communications poursuivent les objectifs suivants :

- assurer la protection des informations sur les réseaux et leurs systèmes de support de traitement de l'information ;
- assurer la maintenance de la sécurité des informations transférées au sein d'une organisation et avec toute entité externe.

11. Développement et maintenance de système

Proximus tient compte, dans ce qu'elle conçoit, de l'impératif de sécurité. Nos experts en sécurité et en respect de la vie privée collaborent avec des équipes de développement, mettent à jour le code et s'assurent que les produits utilisent des protections d'un niveau de sécurité élevé.

Les contrôles de développement et de maintenance de systèmes poursuivent les objectifs suivants :

- s'assurer que la sécurité de l'information fasse partie intégrante des systèmes d'information sur l'ensemble du cycle de vie. Ce point inclut aussi les exigences liées aux systèmes d'information fournissant des services via des réseaux publics ;
- veiller à ce que la sécurité de l'information soit conçue et mise en œuvre pendant le cycle de développement des systèmes d'information ;
- veiller à la protection des données utilisées à des fins de test.

12. Relations avec les fournisseurs

Les contrôles des relations avec les fournisseurs poursuivent les objectifs suivants :

- assurer la protection des actifs de l'organisation auxquels peuvent accéder les fournisseurs ;
- maintenir un niveau convenu de sécurité de l'information et de fourniture de service conforme aux accords de fournisseur.

De manière plus détaillée, Proximus limite l'accès à vos données d'entreprise au personnel de Proximus qui en a besoin pour effectuer son travail, par exemple lorsqu'un agent du service à la clientèle vous aide à gérer vos données.

Des contrôles d'accès renforcés sont instaurés par l'entremise de mesures de protection organisationnelles et techniques. Et lorsque nous collaborons avec des tiers, par exemple des fournisseurs de support à la clientèle, pour fournir des services de Proximus, nous leur faisons signer un document d'annexe de sécurité spécifiant clairement les exigences de sécurité de Proximus et procédons à un audit par coup de sonde pour nous assurer qu'ils fournissent le niveau de sécurité et de respect de la vie privée requis pour se voir accorder l'accès aux données de votre entreprise.

13. Gestion des incidents liés à la sécurité de l'information

Les contrôles de gestion des incidents liés à la sécurité de l'information ont pour but d'assurer une approche cohérente et efficace de cette gestion, y compris la communication consacrée aux événements de sécurité et aux points faibles.

La surveillance de la sécurité et la réponse aux menaces figurent parmi les services de base proposés par le Proximus Cyber Defense Center et l'équipe CSIRT.

Le processus de surveillance et de réaction en matière de sécurité a été établi au sein de Proximus pour atteindre les objectifs clés suivants :

- fourniture de lignes directrices pour la prise de décisions associées aux incidents de sécurité ;
- fourniture d'un cadre de procédure pour une surveillance efficace de la sécurité 24 h sur 24 et 7 j sur 7 (niveau 1) et service de garde de réaction (niveau 2 et supérieur) au sein de Proximus, centrés sur la détection initiale, l'analyse et la réaction ;
- fourniture de lignes directrices pour la prioritisation et l'escalade des incidents de sécurité ;
- mise à la disposition de Proximus et de ses clients des avantages suivants :
- résolution globale améliorée des incidents via un traitement cohérent et dans les délais de la surveillance, de l'analyse, de l'identification et de l'escalade des incidents de sécurité ;
- service amélioré via des interfaces de travail définies avec toutes les équipes impliquées dans le traitement des incidents ;
- rapports améliorés et cohérents, afin de faciliter une amélioration continue de la sécurité chez Proximus.

Proximus, conformément aux normes et exigences internationales de sécurité, a une politique de sécurité en matière d'enregistrement. Cette politique définit toutes les données pertinentes à envoyer à la plateforme SIEM de Proximus pour surveiller avec précision les événements de sécurité.

14. Conformité

Les objectifs de contrôle de conformité sont les suivants :

- éviter les manquements aux obligations légales, statutaires, réglementaires ou contractuelles liées à la sécurité de l'information et à toutes exigences en matière de sécurité ;
- veiller à ce que la sécurité de l'information soit mise en œuvre et exploitée conformément aux politiques et procédures de l'organisation.

* * *