



Thomas Gertsch

Responsable du département Information  
and Communications Technology



Fritz Liechti,

Chef de projet sécurité de l'information

## Cours de sensibilisation à la sécurité de l'information

*Il est évidemment primordial pour une entreprise de mettre en place des solutions lui permettant de protéger son système d'information contre les risques internes et externes. Mais il est tout aussi important de prendre en compte le facteur humain si l'on veut éviter de gros soucis de sécurité.*

*Comment éviter que les collaborateurs soient à l'origine d'incidents de sécurité ? Comment faire comprendre aux utilisateurs la raison de mesures de sécurité parfois contraignantes, parfois impopulaires ? Comment les associer de manière constructive à une démarche essentielle pour l'entreprise ?*

Une entreprise est confrontée à ce problème: Energie Ouest Suisse (EOS), leader en Suisse dans le domaine de la production, du transport et de la commercialisation de l'énergie électrique.

La société Energie Ouest Suisse SA a été créée en 1919 afin d'assurer l'utilisation rationnelle et intensive des forces hydrauliques de la région. La création d'EOS Holding en 2002, pour répondre à de nouveaux objectifs stratégiques, a représenté un changement majeur dans la politique et le fonctionnement de l'entreprise. Aujourd'hui, EOS est l'un des sept exploitants du réseau suisse de transport d'électricité à très haute tension (THT) et prévoit de fusionner avec la société Atel afin de développer encore ses activités sur les marchés suisses et européens. Cette fusion, ainsi que la libéralisation prochaine du marché de l'électricité, posent à l'entreprise de nombreux défis opérationnels, en particulier au niveau des infrastructures et des systèmes qui gèrent l'équilibre entre la demande d'électricité et l'offre disponible.

Thomas Gertsch, Responsable du département Information and Communications Technology, et Fritz Liechti, Chef de projet sécurité de l'information, expliquent pourquoi EOS a choisi de sensibiliser ses 250 collaborateurs aux risques liés à une utilisation inadéquate des systèmes informatiques et de communications.

La sécurité est très importante pour EOS. Thomas Gertsch expose la situation ainsi: "Même si EOS ne compte que 250 collaborateurs, nous sommes très exposés en raison des conséquences que peut avoir un problème de fonctionnement. Tout le monde se souvient de la panne géante qui a touché plusieurs régions d'Europe en novembre 2006 suite à une défaillance en Allemagne. De plus, EOS Trading, notre société qui traite en bourse des produits standards et structurés liés à l'électricité, est soumise aux règles très strictes de la Commission fédérale des banques (CFB). Nous sommes donc légalement tenus d'assurer la sécurité

---

*"Nous voulions montrer aux utilisateurs pourquoi la sécurité et ses contraintes sont nécessaires et favoriser la naissance d'une attitude responsable."*

---



Lac et barrage de l'Hongrin

---

*Il est rare que des actes délibérés provoquent des incidents de sécurité; ils sont plutôt dus à un manque de connaissances ou à une certaine négligence.*

---



La salle des turbines à Chandoline

---

*"Notre but était d'organiser une campagne de sensibilisation vraiment réaliste, qui ne se limite pas à la théorie – c'est inefficace - mais comporte aussi des démonstrations pratiques."*

---

et la traçabilité de nos activités." Fritz Liechti souligne que l'approche sécuritaire de l'entreprise est conçue et conduite de manière stricte: "Notre politique de sécurité repose sur la norme ISO 17799. Elle comporte trois volets: la sécurité opérationnelle, déjà implantée; la surveillance; et enfin, l'aspect humain. C'est là que nous avons fait appel à la collaboration de Navixia."

Pourquoi EOS éprouvait-elle le besoin de mettre en place une campagne de sensibilisation ? Thomas Gertsch: "Le maillon faible de la sécurité, c'est l'homme. En Suisse, nous sommes trop positifs, trop confiants, nous n'envisageons pas volontiers les dangers liés à l'informatique. La culture d'entreprise qui prévalait, avant la création d'EOS Holding, autorisait une grande liberté individuelle. La sécurité étant stricte par nature, il est difficile de l'implanter dans un environnement trop souple. Un contrôle est souvent perçu comme un manque de confiance. Nous voulions montrer aux utilisateurs pourquoi la sécurité et ses contraintes sont nécessaires et favoriser la naissance d'une attitude responsable."

Il est rare que des actes délibérés provoquent des incidents de sécurité; ils sont plutôt dus à un manque de connaissances ou à une certaine négligence. Il est donc dans l'intérêt de toute entreprise de sensibiliser son personnel à la sécurité du système d'information. Fritz Liechti souligne un point particulièrement important pour assurer un bon déroulement du projet et un climat de collaboration positif: "Nous avons demandé une prise de position de la Direction générale avant le lancement du projet et nous avons obtenu son support total, ce qui est indispensable." En particulier, l'introduction aux séances de sensibilisation à la sécurité devrait idéalement être faite par un membre de la direction afin de convaincre les participants de l'implication des dirigeants dans cette démarche importante.

Une formation type dure deux à trois heures et se déroule au sein de l'entreprise. Elle associe la théorie et des démonstrations d'attaques servant à illustrer les dangers encourus. Thomas Gertsch: "Notre but était d'organiser une campagne de sensibilisation vraiment réaliste, qui ne se limite pas à la théorie - c'est inefficace - mais comporte aussi des démonstrations pratiques. Et nous voulions que cette démarche soit une aide pour les utilisateurs en privé, car nous partons du principe qu'une personne consciente des risques à la maison le sera aussi au bureau."

La formation commence par une introduction présentant les objectifs, les tendances et les différents facteurs de la sécurité du système d'information. Elle se poursuit par le traitement de thèmes tels que gestion des mots de passe, risques liés aux virus, risques liés à l'utilisation de la messagerie, utilisation d'internet, sécurité du poste de travail, responsabilité de l'utilisateur, ingénierie sociale... ou tout autre thème important pour l'entreprise. Enfin, elle s'achève par des questions-réponses.

EOS tenait à ce que la formation soit utile aux utilisateurs aussi hors du cadre professionnel. Fritz Liechti: "Chaque participant a reçu un CD destiné à son utilisation privée, contenant des informations et des logiciels utiles relatifs à la sécurité."

Avant le cours, Navixia et l'entreprise organisatrice doivent prévoir une préparation préalable afin de procéder à un état des lieux, adapter le contenu au public ciblé et déterminer le message précis à faire passer aux utilisateurs lors de la sensibilisation.

---

*"La démarche de sensibilisation a été un succès."*

---




---

*"Aujourd'hui, les collaborateurs réalisent que la sécurité en place est structurée, que son approche est maîtrisée et professionnelle."*

---



**Navixia SA**

Route du Bois 1  
CH - 1024 Ecublens

Tél.:  
41 (0)21 324 32 00

Fax:  
41 (0)21 324 32 01

E-mail:  
info@navixia.com

Web:  
www.navixia.com

Thomas Gertsch: "La grande majorité de nos collaborateurs a suivi la formation, par groupes d'une vingtaine de personnes, entre l'été et l'automne 2006. Le cours était le même pour tous les utilisateurs, mais bien sûr les questions variaient selon le niveau des participants et Navixia a toujours su y répondre de manière claire."

EOS, ayant pris conscience que la charge de travail liée à la sécurité dépassait les possibilités de son équipe informatique en place, avait opéré une sélection serrée pour identifier le partenaire apte à la seconder dans le projet de sensibilisation et par extension dans la gestion de la sécurité de l'information en général. Thomas Gertsch: "De par la nature de notre société (informatique transactionnelle et temps réel), il nous fallait un partenaire possédant les compétences théoriques et surtout pratique, doté d'une grande souplesse et n'offrant pas uniquement des solutions standardisées. Nous avons établi un cahier des charges très détaillé comportant six critères de compétence pour identifier le partenaire idéal. L'un de ces critères était sa capacité à sensibiliser notre personnel, car la mise en place de la sécurité demandait un important changement de mentalité en interne. Pour nous, la campagne de sensibilisation devait faire la preuve de la qualité de notre partenaire et représenter le point de départ de notre collaboration future. Elle devait aussi montrer à nos collaborateurs que notre sécurité est élaborée de manière réfléchie avec un partenaire compétent."

Quel a été l'impact de la formation ? Thomas Gertsch est positif: "La démarche de sensibilisation a été un succès. Avant la formation, les réactions en interne étaient passablement mitigées. Les utilisateurs s'attendaient soit à s'ennuyer, soit à entendre des évidences... Beaucoup ensuite ont trouvé le sujet intéressant."

Fritz Liechti ajoute: "La formation n'a pas fait effet d'un jour à l'autre, mais les utilisateurs ont pris conscience de la réalité des dangers. Ils ont aussi vu que nous avons un partenaire compétent pour la sécurité et que nous traitons les points à risques les uns après les autres. Le faire sans perturber l'opérationnel prend du temps et beaucoup d'attention. Aujourd'hui, les collaborateurs réalisent que la sécurité en place est structurée, que son approche est maîtrisée et professionnelle."

MM. Gertsch et Liechti sont donc satisfaits du déroulement de la campagne de sensibilisation et des prestations de Navixia. Thomas Gertsch: "La même formation sera dispensée à tous les collaborateurs qui ne l'ont pas encore suivie. Nous prévoyons aussi d'organiser un nouveau cours portant sur des thèmes plus spécifiques, tels que l'informatique mobile, etc. Notre but est d'organiser, au moins tous les deux ans, un cours sur un thème particulier. Navixia a absolument répondu à nos attentes. Nous apprécions sa disponibilité, sa réactivité et sa compétence."

*De manière générale, Navixia recommande de mettre l'utilisateur au centre de la stratégie sécurité de l'information de l'entreprise, non seulement en l'informant régulièrement sur ce qui est permis ou interdit à l'utilisateur du système d'information de la société, mais aussi en le sensibilisant aux risques liés à une utilisation inadéquate des systèmes informatiques et de communications. C'est seulement ainsi que l'utilisateur pourra devenir un partenaire responsable de la politique de sécurité de l'entreprise.*