LES DOSSIERS TECHNIQUES

Fiches pratiques sécurité TPE

Sécurité réseaux

Mai 2016

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Stéphane	**MAKOWSKI**	*Ministère de la défense*

Les contributeurs :

Michel	**BERTIN**	*Individuel*
Paul	**CONSTANT**	*Individuel*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

Fiches pratiques sécurité TPE	
SÉCURITÉ RÉSEAUX	**RESOxx**

Objectif

Présenter sous forme de fiches pratiques des préconisations pour sécuriser le poste de travail informatique et son environnement.

Public concerné

Tout utilisateur de l'outil informatique, travailleur indépendant ou personnel d'une petite entité (PME, TPE, profession libérale) ou simple particulier.

Utilisation du référentiel

Chaque fiche traite un sujet précis et peut être consultée indépendamment.
Ce référentiel est structuré par thèmes.

Contenu du thème

N° de Fiche	Titre de la fiche	Descriptif simplifié et résumé du sujet
RESO01	Sécurisation des échanges	Comment protéger les données échangées et assurer une connexion sécurisée entre les équipements.
RESO02	Architecture réseau local	Comment vérifier que les points essentiels d'un réseau IP (Internet Protocol) sont correctement configurés et paramétrés.
RESO03	Poste isolé connecté à Internet	Comment sécuriser un poste isolé connecté à Internet contre les infections informatiques.
RESO04	Pare-feu (Firewall)	Comment sécuriser le réseau de l'entreprise contre des intrusions malveillantes (par exemple réseau de l'entreprise et Internet).
RESO05	Messagerie	Comment protéger les informations contenues dans les messages, de toute altération touchant à la confidentialité, l'intégrité mais aussi à la non-répudiation ou la preuve.
RESO06	Web	Comment contrôler l'utilisation du Web et veiller à ce qu'elle ne contrevienne pas à la politique de sécurité.

SÉCURITÉ RÉSEAUX	
Sécurisation des échanges	**RESO01**

Contexte

Dans les échanges de données en réseau, les informations circulent souvent en l'absence de toute sécurisation. Aujourd'hui les volumes d'échanges sont considérables.

En cas d'interception ou d'écoute illicite, les informations non protégées peuvent facilement être exploitées et ainsi porter atteinte à leur confidentialité.

Objectifs

- Protéger les données sensibles transitant sur les réseaux en assurant un chiffrement des fichiers, des répertoires (ou dossiers) et des programmes ;
- assurer une connexion sécurisée entre les équipements en utilisant la cryptographie (qui consiste à chiffrer, signer et authentifier les données).

Recommandations

- Utiliser un logiciel de messagerie permettant l'envoi de messages chiffrés (contenu ou/et pièce(s) jointe(s)) ;
- procéder, dans le cas où la messagerie n'est pas capable de chiffrer le contenu, au chiffrement local des informations sensibles qui figureront en pièce jointe ;
- mettre en œuvre des liens sécurisés (VPN : réseau privé virtuel...) pour tous les échanges qui sortent du réseau de l'entreprise (accès de type Extranet, prise de contrôle à distance...) ;
- changer les accès d'authentification (login/mot de passe) usine des équipements réseaux et de sécurité (par exemple Cisco/Cisco) et les modifier régulièrement (en particulier lors du départ de salariés y ayant eu accès).

Remarques

- Noter que :
  - la robustesse du chiffrement est dépendante de l'algorithme de chiffrement utilisé, de la longueur des clefs utilisées et de sa non-vulnérabilité relative aux failles de sécurité publiées (logiciel à jour des correctifs publiés) ;
  - pour réduire le risque d'écoute (confidentialité) et éventuellement de modification (intégrité) des données dans les réseaux locaux (LAN), l'utilisation de commutateurs Ethernet (Switch) permet une meilleure sécurisation ;
  - dans la mesure où la fonction existe dans le commutateur, y activer l'anti-usurpation d'adresses MAC (antispoofing) pour empêcher les attaques de type « homme du milieu » ;
  - la mise en œuvre d'un réseau local virtuel (VLAN) permet de créer un ensemble logique isolé pour améliorer la sécurité au sein d'un même réseau physique ;
  - il existe des solutions standard pour chiffrer les données (se référer à la fiche LOGI02 sur le chiffrement).

SÉCURITÉ RÉSEAUX	
Architecture réseau d'entreprise	**RESO02**

Contexte

Le travail en réseau est devenu incontournable. Les réseaux sont constitués par des équipements de différentes technologies (y compris de télécommunications comme les IPBX), raccordés entre eux selon des architectures variées.

Objectif

Vérifier si les points énumérés en recommandations sont correctement configurés et paramétrés, en particulier dans la perspective (éventuelle) de raccordement du réseau interne à Internet ou de la mise en œuvre de solutions globales de sécurité.

Recommandations

1) Dans les relations en interne :

- éviter l'emploi de technologies différentes ;
- segmenter le réseau en plusieurs sous-réseaux (physiques ou logiques), interconnectés par des commutateurs ou des ponts/routeurs associés à des équipements de sécurité (pare-feu classique, UTM, détection et prévention d'intrusion IDS/IPS…), par exemple en suivant l'organisation de l'entreprise ;
- ne laisser ouvert sur la pare-feu que les protocoles utilisés ;
- gérer les droits d'accès sur les répertoires ;
- proscrire les partages des ressources de poste à poste au bénéfice d'un (de) serveur(s) de fichiers administré(s) et sécurisé(s) ;
- disposer en permanence d'un inventaire des équipements autorisés et des moyens de contrôler la connexion d'autres équipements.

2) Dans les relations avec l'extérieur :

- utiliser des plages d'adresses privées non routables sur Internet ;
- doubler la liaison avec Internet (abonnement avec un autre prestataire) pour assurer une meilleure disponibilité de service ;
- prévoir un équipement de sécurité pour le filtrage de ports et un serveur de log ;
- implémenter un dispositif de protection robuste (antivirus + pare-feu + proxy exigeant une authentification individuelle + détection d'intrusion) cohérent (performances et flux à traiter) ;
- éviter d'accéder à la fois au Web et à des données critiques de l'entreprise via le même poste.

Remarques

- Un audit de conformité systématique du réseau (inventaire, contrôle de tous les équipements, des configurations et des paramètres réseaux, tests d'intrusion), si possible annuel, permettra de valider le bon respect des choix et recommandations précédentes ;
- privilégier des contrôles par automatismes à la demande ou programmés – même succincts – pour une meilleure réactivité en cas de détection d'anomalies ;
- privilégier un point d'accès unique et sécurisé à Internet (routeur + pare-feu + antimalware).

SÉCURITÉ RÉSEAUX	
Poste isolé connecté à Internet	**RESO03**

Contexte

Il s'agit de considérer le cas d'un micro-ordinateur connecté à Internet quel que soit le moyen d'accès utilisé (ADSL, 3G…), qu'il soit fixe ou mobile.

Objectif

Sécuriser une telle configuration contre les codes malveillants et les intrusions.

Recommandations

- Ne pas installer et désactiver les services du système d'exploitation que vous n'utilisez pas ;
- s'assurer que les logiciels installés proviennent de sources sûres (supports d'origine ou du site officiel de l'éditeur ou de l'auteur, dont l'empreinte d'intégrité fournie peut être vérifiée) et sont adaptés aux besoins de l'entreprise ;
- vérifier périodiquement (au minimum une fois par an) que les logiciels installés sont bien à jour (nouvelle version, application des correctifs) ;
- désactiver le compte « invité » ;
- paramétrer le système et les logiciels de façon à empêcher tout automatisme au niveau de l'exécution des scripts, de l'ouverture des fichiers attachés aux messages, des téléchargements et des supports amovibles ;
- faire en sorte que l'avis de l'utilisateur soit systématiquement requis par le système ;
- privilégier les comptes utilisateurs avec des droits limités ;
- n'utiliser le compte « administrateur » ou « root » que pour administrer ;
- mettre en place un mot de passe de session complexe et robuste à modifier régulièrement par l'utilisateur.
- installer un antivirus et s'assurer que la mise à jour régulière du fichier de signature et du moteur fonctionne convenablement ;
- installer un logiciel de type « pare-feu individuel » permettant de contrer les tentatives d'intrusion ou souscrire auprès du fournisseur d'accès l'option de sécurité adéquate ;
- prévoir une solution de sauvegarde et de restauration du poste (système, données…) sur les moyens usuels (serveur, support amovible, cloud...).

Remarques

- Utiliser un système d'exploitation intégrant de véritables mécanismes permettant le contrôle d'accès aux ressources ;
- prendre en compte que l'installation « par défaut » de ces systèmes peut induire des failles de sécurité ;
- se référer pour les points particuliers ou spécifiques, à la documentation des éditeurs (ou auteurs) des logiciels et systèmes d'exploitation, ainsi qu'à leurs sites Web officiels, pour prendre connaissance des paramétrages les plus appropriés et des correctifs les plus récents ;
- procéder de préférence à des tests de validation du niveau de sécurité de la configuration par un intervenant qualifié si les données manipulées s'avèrent sensibles pour l'entreprise ;
- privilégier l'installation d'une suite de sécurité de sécurité offrant la possibilité de se mettre à jour sur Internet et contrôlable à distance depuis le réseau d'entreprise ;
- utiliser les fonctionnalités de filtrage des équipements de connexion à Internet lors de leur configuration.

SÉCURITÉ RÉSEAUX	
Pare-feu (Firewall)	**RESO04**

Contexte

Il s'agit de renforcer le contrôle, la maîtrise et la traçabilité des échanges entre les réseaux internes de l'entreprise d'une part et les réseaux externes d'autre part dont Internet.

Objectif

Éviter que des échanges soient à l'origine d'intrusions extérieures ou contraires aux règles de l'entreprise.

Recommandations

Cette fiche entend se limiter aux aspects pratiques à ne pas négliger, à savoir :

- définir en entrée comme en sortie la règle a minima suivante : « tout ce qui n'est pas explicitement autorisé est interdit » ;
- mener une étude rigoureuse des besoins en constituant une matrice de flux qui conduit à la mise en place des règles de sécurité (quels accès, quels services, quelle politique de sécurité…) ;
- appliquer les recommandations pour l'adressage privé IP (voir fiche RESO02) ;
- s'assurer que le prestataire de services et le système choisis présentent au minimum les références suivantes :
  - personnel intervenant certifié par l'éditeur ;
  - contrat de service assurant la prise en compte des évolutions et des mises à jour et, si nécessaire, la formation des intervenants locaux ;
  - en cas de télémaintenance, utilisation de moyens d'authentification forte (au moins 2 paramètres), de chiffrement de la liaison et d'un filtrage sur la ou les adresses IP d'intervention ;
  - installer le dispositif pare-feu sur un équipement dédié et dans un local sécurisé, dont les accès sont strictement contrôlés ;
- vérifier que le dispositif est conforme aux spécifications du cahier des charges. Cette vérification peut être complétée par un audit externe de sécurité ;
- sauvegarder régulièrement (au minimum une fois par an), les règles, les configurations et les journaux (logs) de l'ensemble du mécanisme de protection (pare-feu, équipements de filtrage...) conformément à la législation ;
- intégrer ce dispositif dans le plan de reprise d'activité ;
- bloquer tout accès non sécurisé à une console d'administration depuis internet ;
- suivre, en ce qui concerne l'administration, les recommandations des fiches ADMI01, ADMI02, ADMI03 et ADMI04 disponibles sur le site du CLUSIF.

Remarque

Utiliser si possible, un outil d'analyse pour faciliter l'exploitation des fichiers « log ».

SÉCURITÉ RÉSEAUX	
Messagerie	**RESO05**

Contexte

Les échanges de messages entre utilisateurs ne cessent d'augmenter en nombre, en volume et en criticité des contenus. Ces échanges sont de plus en plus la cible de nombreuses intentions malveillantes.

Objectif

Protéger les informations contenues dans les messages, de toute altération touchant non seulement à la confidentialité, l'intégrité et à la disponibilité, mais aussi à la non répudiation ou la preuve.

Recommandations

- Disposer d'un moyen de chiffrement robuste pour assurer la confidentialité des échanges ;
- disposer d'un moyen d'identification, d'authentification par signature ou certificat de l'émetteur d'un message ;
- intégrer dans la politique de sécurité de l'entreprise les différentes fonctions de sécurité présentes dans la ou les applications de messagerie ;
- mettre en place un service centralisé de vérification et de contrôle du contenu des messages afin d'éradiquer toute malveillance (outil antispam par exemple).

Remarques

- Consulter la fiche pratique rédigée par la CNIL sur le contrôle de l'utilisation de la messagerie ;
- vérifier auprès du correspondant informatique et liberté de l'entreprise ou de la CNIL la conformité des opérations liées aux contrôles ;
- rédiger une charte d'utilisation de la messagerie (aspects techniques et juridiques) ;
- informer les instances représentatives du personnel de la mise en place des moyens de contrôle de la politique de sécurité ;
- veiller à ce que la messagerie (données, programmes, serveurs et clients) suive les mêmes règles que toute autre application nécessitant un haut niveau de disponibilité ;
- sensibiliser les utilisateurs sur les règles d'usage (conditions d'accès, contrôles, conservation des traces…) et en particulier :
  - être sensibilisé au fait que les messageries sont à la fois victimes et propagatrices de malveillances (spam, virus, vers, chevaux de Troie, malware…) ;
  - être conscient que la messagerie n'est pas un lieu de stockage et n'a pas pour vocation d'archiver ou de sauvegarder les messages et les pièces jointes ;
  - être respectueux des bonnes pratiques (éviter les chaînes de messages, ne pas ouvrir un mail douteux, ne pas cliquer sur un lien suspicieux...).

Contexte

Celui d'un réseau connecté à Internet avec des utilisateurs devant accéder aux multiples ressources du Web.

Objectif

Contrôler l'accès au Web et son utilisation en veillant à ce qu'ils ne contreviennent pas aux lois et à la politique de sécurité.

Recommandations

Parmi les outils existants, il existe le relais mandataire sécurisé (proxy) et des outils spécialisés d'analyse de contenu, qui permettent de :

- réaliser le paramétrage adéquat pour :
  - identifier et authentifier les utilisateurs autorisés à accéder au Web ;
  - interdire ou autoriser l'accès à certains sites (filtrage possible en fonction de listes noires, blanches ou grises) ;
- contrôler la liste des adresses web (URL) accédées par les utilisateurs en analysant de manière générale les fichiers « logs » générés par le proxy et en vérifier la conformité avec la politique de sécurité ;
- améliorer les performances par la mise en mémoire des pages HTML les plus consultées (fonction cache) ;
- conserver les logs de transaction sur une durée conforme à la législation en vigueur ;
- protéger les adresses IP internes des utilisateurs (translation d'adresses IP) ;
- compléter la détection des infections logiques (virus, vers…).

Remarques

- Consulter la fiche pratique rédigée par la CNIL sur le contrôle de l'utilisation d'Internet ;
- vérifier auprès du correspondant informatique et liberté de l'entreprise ou de la CNIL la conformité des opérations liées aux contrôles ;
- rédiger une charte d'utilisation du web (aspects techniques et juridiques) ;
- informer les instances représentatives du personnel de la mise en place des moyens de contrôle de la politique de sécurité ;
- sensibiliser les utilisateurs sur les règles d'usage (conditions d'accès, contrôles, conservation des traces…).