LIVRE BLANC ITRUST

Retour d'experience des experts ITrust

10 failles de sécurité correspondent à 99% des failles de sécurité dans les entreprises

Rédigé par ITrust

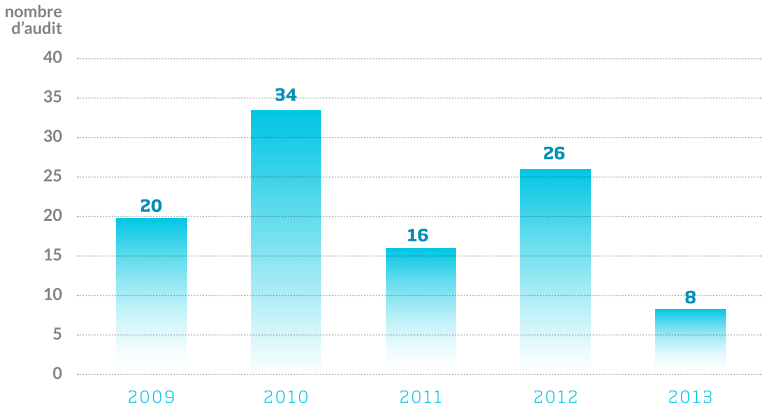
Novembre 2013 sur la base des 5 dernières années d'audit de l'équipe d'audit intrusif d'ITrust.

ITrust
IT Security Services

Introduction

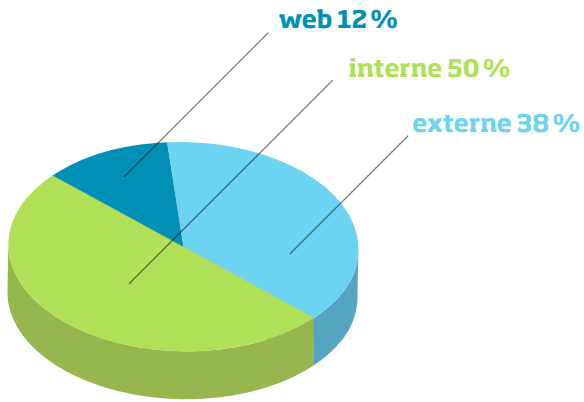
Ce n'est pas une surprise, l'année écoulée a encore été riche en actualité concernant la cybercriminalité. Cette criminalité est d'ailleurs devenue un enjeu stratégique pour les états qui ne sont pas non plus à l'abri de cette menace. On se souvient notamment du piratage très médiatisé de l'Élysée [1].
75% c'est le nombre d'entreprises piratées au cours des deux dernières années selon une étude du Cenzic[2]. Ce chiffre atteint même les 90% sur les statistiques des tests d'intrusion menés par ITrust chez nos clients.

Durant ces cinq dernières années, les consultants du pole «pentest» (audit intrusif) d'ITrust sont intervenus une centaine de fois pour réaliser des tests d'intrusions chez nos clients.



Répartition du nombre d'audit par an
Total : 104 audits

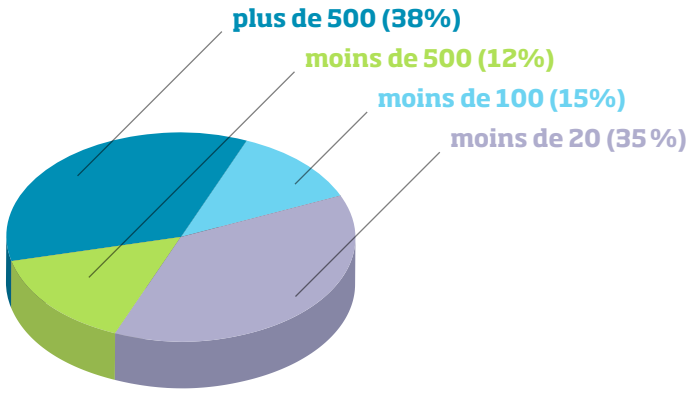
Ces tests sont aussi bien réalisés en interne, en externe pour tester les services du client en DMZ ou encore sur de simples sites web. Voici la répartition des ces différents tests.



Répartition du type d'audit réalisé

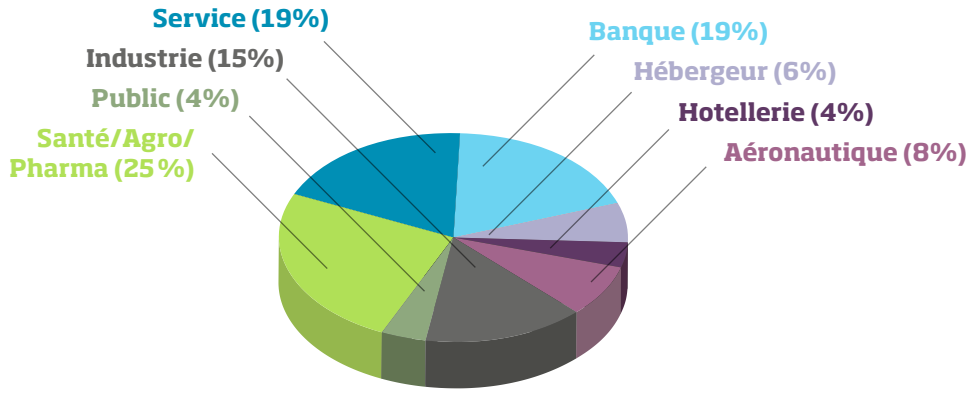
Dans le but d'apporter un éclairage objectif sur la pertinence de ce palmarès, nous nous sommes attachés à constituer des statistiques sur l'échantillon de données que nous traitons.

Ainsi nous fournissons les informations sur la structure :



Répartition des clients par nombre d'employés

Et le domaine d'activité de nos clients:



Répartition des clients par domaine d'activité

Cet article dresse le panorama des 10 vulnérabilités les plus rencontrées lors de nos audits accompagnés d'études de cas. C'est donc un retour d'expérience concret sur les 5 dernières années d'expérience des équipes techniques d'ITrust.
Lors de nos audits ou des interventions sur incidents réalisées par ITrust, 99% des systèmes ont été compromis par au moins une de ces 10 failles.

Retour d'expérience : le top 10 des vulnérabilités rencontrées

Corriger ces 10 vulnérabilités essentielles permettrait d'élever grandement le niveau de sécurité d'une organisation.

10 SYSTÈMES TROP VERBEUX : *le salon de thé du réseau*

Cette vulnérabilité n'en est pas vraiment une en soi, mais elle est souvent l'étape initiale lors d'un test d'intrusion. Même si cette faille ne permet pas de compromettre directement un système, elle permet de récolter un tas d'informations utiles – notamment dans le cadre de la découverte de cibles intéressantes.

Dans la catégorie des grands bavards, on retrouve les deux principaux serveurs :

Serveurs DNS "Système de nom de domaine"

Le DNS est un service utilitaire primordial pour le bon fonctionnement des services applicatifs comme la navigation ou la messagerie. Les portes sont souvent laissées grandes ouvertes sur l'ensemble du réseau.
Les attaquants font alors appel au transfert de zone pour lister l'ensemble des machines du domaine. Cette démarche permet de découvrir rapidement les cibles intéressantes - par responsabilité ou département (R&D, comptabilité)

Contrôleur de domaine trop verbeux

Les domaines trop verbeux fournissent aux attaquants des informations cruciales pour organiser leurs attaques. Que se soit au travers de connexions LDAP ou Samba, il est souvent possible d'obtenir des informations intéressantes comme le nom de domaine, la version du système d'exploitation (fingerprint) et encore plus intéressant la liste des utilisateurs du domaine.

Étude de cas : récupération des utilisateurs d'un domaine.

Utilisation de la commande rpcclient sur un doamine windows :

```
# > rpcclient 192.168.1.1 -p 139 -U% -c enumdomusers
        session request to 192.168.0.4 failed (Called name not present)
        user:[Administrateur] rid:[0x1f4]
        user:[Invité] rid:[0x1f5]
        user:[Compta] rid:[0x476]
        user:[Commercial] rid:[0x4c3]
```

Utilisation pour obtenir les administrateurs du domaine

```
# > rpcclient 192.168.0.4 -p 139 -U% -c 'querygroupmem 0x200'
        session request to 192.168.0.4 failed (Called name not present)
        rid:[0x1f4] attr:[0x7]
```

De la même façon, il est possible d'obtenir au niveau de chaque machine, l'utilisateur connecté

9 RELATIONS DE CONFIANCE : *propagation de la compromission*

En environnement UNIX, les programmes de terminaux à distance (rlogin et rsh) utilisent un système d'authentification faible et permettent en plus de mettre en place des relations de confiance entre machines (par l'intermédiaire de fichier .rhosts ou hosts.equiv). Ainsi si l'une des machines est compromise, l'attaquant peut se connecter librement à l'ensemble des machines de confiance. Ces applications sont dans la plupart des cas interdites dans la politique de sécurité au profit d'outil plus sécurisée comme SSH. Mais là encore, l'expérience montre que des rebonds sont possibles à cause du manque de protection des clés privées. La clé publique associée est souvent utilisée sur un grand nombre de serveurs permettant à l'attaquant de s'y connecter.

En environnement Windows, il est possible de définir des relations de confiance entre domaines Active Directory. Dans ce cas, l'annuaire des utilisateurs est répliqué entre domaines de confiance. Un attaquant s'il arrive à obtenir un compte sur un domaine «plus faible» aura accès à tous les domaines avec compte.

8 GESTION DES DROITS : *besoin d'en connaitre*

Le besoin d'en connaitre est une notion primordiale en sécurité pour s'assurer de la confidentialité des données. Bien souvent la gestion des droits sur les partages de fichiers présente des faiblesses : des restrictions d'accès trop laxistes, voire inexistants, permettent d'obtenir de nombreuses informations stratégiques et confidentielles.

Étude de cas : le test du stagiaire.

Dans la plupart des structures Active Directory, les utilisateurs appartiennent à des groupes et les partages sont ouverts à certains groupes. Un stagiaire est ajouté au groupe de son (voire ses) maitre de stage.
Le test consiste à laisser le stagiaire voir ce qu'il peut obtenir comme information. L'expérience montre qu'à la suite de ce test, la personne aura au moins obtenu des informations confidentielles et dans la plupart des cas des informations sur les comptes utilisateur lui permettant de devenir administrateur d'un serveur.

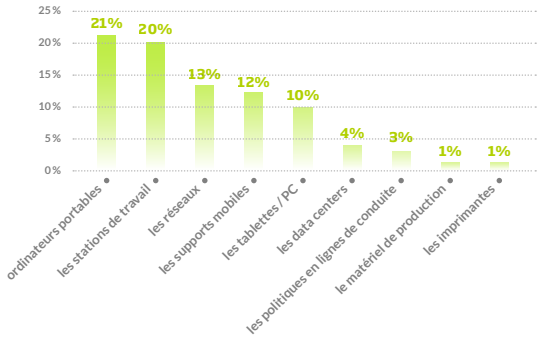
Les employés sont le maillon faible dans la chaine de sécurité informatique. Ils représentent 50% des menaces en sécurité.

7 PROTOCOLES D'ADMINISTRATION : *le diable est dans les détails*

Même dans les entreprises où la sécurité est prise en compte sur les postes utilisateurs et les serveurs, certaines catégories d'équipements passent quasiment tout le temps à la trappe. Que ce soit les éléments actifs du réseau comme les switchs ou les routeurs ou les imprimantes, la sécurité est souvent négligée. Ainsi les mots de passe d'administration par défaut sont rarement changés et s'ils le sont, il reste les protocoles d'administration activés par défaut sur ce genre d'équipement.
La présence de protocoles non sécurisés qui font transiter les mots de passe en clair constitue aussi une source très importante de vecteurs d'attaques : prenons par exemple : FTP, Telnet, …

Étude de cas : SNMP sur un routeur d'agence
Le cas s'est présenté lors d'un de nos audits. Un routeur VPN d'une agence du client dispose du service SNMP activé et en écoute sur internet. La configuration par défaut permet de lire et surtout d'écrire les informations de la MIB. Le scénario mis en place a consisté à rediriger les requêtes DNS sur un de nos serveurs et étudier les statistiques des requêtes. Cette première étape concluante, le trafic intéressant est redirigé vers notre serveur et très rapidement l'accès au compte de messagerie ainsi que l'intégralité des messages transitant est recueillie par nos soins.

Bien que le matériel de production et imprimante ne représente que 1% des menaces en sécurité informatique, elles sont souvent bien trop négligées.



Étude de cas :
Arrêt de la production
Le SNMP n'est pas le seul protocole d'administration ouvert. Prenons le cas d'un onduleur sur les chaines de production d'un client. Cet onduleur est en configuration «usine», il suffit donc de se connecter sur le serveur web d'administration avec les comptes par défaut pour avoir la possibilité d'éteindre tous les serveurs de production.

6 BASE DE DONNÉES

Les bases de données sont une cible de choix, car elles renferment beaucoup d'informations utilisables. Lorsque les mots de passe par défaut sont changés, les administrateurs des bases de données administrant un grand nombre de serveurs utilisent souvent des mots de passe faibles qui sont fonction du nom du serveur.
Au-delà des informations confidentielles contenues, ces bases contiennent des listes d'utilisateurs dont il est facile d'obtenir les mots de passe par cassage. Ces comptes peuvent alors être réutilisés pour continuer l'attaque sur le réseau.

Étude de cas : L'ERP une cible parfaite.
Dans ce cas, la société autorisait les commerciaux à avoir une instance de l'ERP sur leur poste pour pouvoir l'utiliser en clientèle. Le service de base de données écoutant sur le réseau, il ne fallut que peu de temps pour trouver le mot de passe évident et obtenir la liste des clients de la société et les propositions associées - un vrai trésor très profitable à la revente pour un attaquant.

gamigo games

Nous constatons, aujourd'hui que le piratage de base de données correspond à 14% des menaces en sécurité.
http://buff.ly/11umuYS
La base de données de Gamigo fut piratée en 2012.

5 PARTAGE DE FICHIERS

De nombreux systèmes peuvent avoir des partages de fichiers. Ces partages peuvent être gérés via différents protocoles (FTP, NFS, SMB,...). Les restrictions sur ces partages sont en général trop faibles, voire inexistantes. Que ce soient les accès anonymes autorisés sur un FTP ou la restriction d'accès au réseau d'entreprise pour les partages SMB ou NFS, un attaquant a la possibilité d'obtenir énormément d'informations confidentielles. Le pouvoir de nuisance est extrêmement important lorsqu'un attaquant décide d'utiliser la technique de la terre brulée et de supprimer tous les fichiers présents (sauvegarde, données financières...).

Étude de cas : L'imprimante de la direction

Sur les toutes les imprimantes récentes, des partages sont activés par défaut pour pouvoir récupérer les scans ou les fax reçus. Dans le cas présent, l'imprimante stockait tous les documents - ainsi il a été possible de retrouver l'ensemble de photocopies, scans et fax de la direction.

http://buff.ly/ZWQ2Mv
Des chercheurs de l'Université
Columbia affirment qu'ils ont découvert une nouvelle classe de failles de sécurité informatique qui pourrait avoir un impact sur des millions d'entreprises, les consommateurs, et même des organismes gouvernementaux. Les imprimantes peuvent être contrôlées à distance par des criminels informatiques sur Internet.

4 SERVEURS À L'ABANDON

Un constat qui est fait lors de nos audits est qu'il n'y a presque jamais d'inventaire matériel ou logiciel réalisé au sein des systèmes d'informations. Lors d'un audit, la découverte de serveurs de tests ou de serveurs à l'abandon, non maintenus et largement vulnérables surprend les administrateurs qui n'avaient même pas connaissance de ces éléments sur le réseau. Ces serveurs sont facilement exploitables et peuvent toujours contenir des informations valides. De plus ils servent de rebond pour attaquer des cibles plus intéressantes.

3 VULNÉRABILITÉS WEB

Cette catégorie pourrait faire l'objet d'un article à part entière tant le sujet est vaste. Les vulnérabilités web ne représentant pas - dans notre cas – la majorité des vulnérabilités rencontrées de par le profil de notre échantillon. Cependant, très souvent lors d'audit de site web, il est possible d'exploiter des vulnérabilités applicatives.

Si on confronte le top 10 des vulnérabilités web fourni par l'OWASP [3] à notre retour d'expérience terrain, voici ce que l'on peut en dire :
Les vulnérabilités que nous rencontrons sont réparties en deux catégories :

Phase 1 : les points d'entrées

Ces vulnérabilités permettent d'avoir un premier accès au système et obtenir des informations. Par ordre de fréquence, on retrouve :

- Les systèmes pas à jour

Cette catégorie de vulnérabilité fait l'objet d'un paragraphe entier du top 10

- Les injections SQL
- Les attaques XSS
- La gestion des sessions

Étude de cas : Vol de session / vidéosurveillance

Une société de sécurité propose à ses clients un système de vidéo surveillance de leurs locaux accessible par internet. Les cookies de sessions ne sont pas protégés et le rejeu est possible. Ainsi, tout utilisateur peut deviner le format des cookies et accéder aléatoirement à la vidéosurveillance d'un autre client. Le problème aurait pu se limiter à la divulgation entre clients si les mots de passe pour se connecter n'avaient pas été aussi faibles. Le système de sécurité se transforme avec peu de ressources en un moyen efficace pour organiser un cambriolage.

Phase 2 : exploitation

Cette catégorie de vulnérabilités permet dans un deuxième temps d'exploiter les informations recueillies dans la première phase. Dans cette catégorie, on retrouve :

- L'exposition de données sensibles
- L'absence de configuration sécurisée
- Le manque de restriction de privilèges.

Une fois que l'on a identifié une vulnérabilité exploitable sur le site, si les privilèges ne sont pas gérés correctement, il est souvent possible de prendre la main sur le serveur et d'obtenir tous les droits. Suivant le potentiel de nuisance de l'attaquant, l'exploitation peut aller du défacage de site, à la perte d'informations (potentiellement sensibles comme des données bancaires), à la constitution d'un zombie voire à la suppression de l'ensemble des données.

Étude de cas : Fonctions PHP non protégées

Les sites web offrant la possibilité d'uploader du contenu (comme des images par exemple) utilisent les fonctionnalités d'upload de PHP. Si des contrôles stricts de ces fonctionnalités ne sont pas mis en place, il est possible d'uploader un web shell et d'obtenir des informations comme les condensés des mots de passe. Ainsi par rebond, il est possible de prendre la main sur le serveur en backoffice.

2 MOT DE PASSE

Chez 96% des clients audités, un mot de passe par défaut ou trivial permet d'accéder à des ressources confidentielles. Un simple stagiaire y arriverait. C'est un sujet pour lequel les utilisateurs sont le plus sensibilisés en entreprise, il reste pourtant l'un des vecteurs d'attaques les plus utilisés et surtout le plus simple à exploiter.

RETOUR D'EXPÉRIENCE :
le top 3 des mots de passe les plus faibles rencontrés

- Le compte n'a pas de mot de passe
- Le mot de passe est le même que le login
- Le mot de passe est le mot de passe générique de création de comptes

Et n'oublions pas le mot de passe et le prénom de l'utilisateur, de ses enfants, un simple mot du dictionnaire....

Étude de cas : Le serveur BlackBerry
Pour illustrer ce problème, nous revenons sur le cas d'un serveur Windows avec le mot de passe de l'administrateur de la base de données laissé par défaut. Cet accès nous permet de créer un utilisateur sur le système et de voir que le serveur BlackBerry ne supprime pas les fichiers temporaires. Des informations très confidentielles sont obtenues par ce biais.

1 FAILLES HISTORIQUES

Ce qui devrait être le problème le plus anecdotique et paradoxalement le plus facile et le plus automatisé à exploiter. Les vulnérabilités historiques sont connues et des correctifs sont fournis par les éditeurs dès qu'elles sont publiées. Il suffit de mettre à jour les systèmes pour s'en prémunir. Cependant, ces vulnérabilités sont le plus grand vecteur d'attaques et d'infections des systèmes d'informations. Les dernières grandes actualités concernant des compromissions d'entreprises concernent des systèmes qui ne sont pas mis à jour depuis des années.
On se souvient du piratage du PlayStation network de Sony. Ce piratage a été permis grâce à une vulnérabilité sur les serveurs web connue et corrigée plusieurs mois avant.

COMPLÉMENT AUX 10 FAILLES

Le top 10 peut être enrichi de 3 failles. Montant le total à 13 failles.

Ce top 13 représente pour nous l'ensemble des failles exploitées exhaustives d'un SI.

> Failles humaines
Exemple : Un collaborateur donne son mot de passe à un faux administrateur système au téléphone

> Failles applicatives

> Failles inconnues

Conclusion

Plus de 9 fois sur 10 nous pénétrons sur un système d'information au cours d'un audit. Et ce à partir d'une faille de sécurité triviale (issue du Top10); depuis une simple connexion internet la plupart du temps. Si nous y arrivons, des pirates, personnes malveillantes ou virus y arrivent aussi.

Alors on fait quoi ?

Souvent nous rencontrons des clients qui empilent des outils de sécurité comme les couches d'un millefeuille alors qu'en supprimant ces 10 failles essentielles, le niveau de sécurité augmenterait exponentiellement. C'est pourquoi il est nécessaire de mettre en place des contrôles permanents pour vérifier ces points. Un rapport de Verizon montrait cette année que 97% des violations de données auraient pu être évités par de simples contrôles [4].

Je suis expert sécurité en informatique depuis 15 ans
J'ai été responsable sécurité salle de marché a la bnp arbitrage
Je suis intervenant expert en ssi cloud à l'Assemblée nationale
Je suis le PDG fondateur de ITrust crée il y a 7 ans

Notre métier est complexe. On y trouve beaucoup de normes et méthodes. Un peu comme en médecine, il y existe un nombre incalculable d'outils, de virus, de méthodes, d'écoles utilisant chacune leur propre protocole/procédure.
C'est un métier jeune, une vingtaine d'années ;
Les nouvelles menaces, notamment les APT et le cloud laissent beaucoup de nos clients dans l'expectative. Peu d'entre eux comprennent pourquoi nous devons toujours 20 ans après continuer à améliorer les systèmes par de nouvelles méthodes et nouveaux outils. Ils constatent avec effarement et incrédulité que les antivirus et firewalls ne sont plus assez efficaces pour les protéger. Ils s'aperçoivent que nombre d'entre nous leur ont menti à leur promettant la fin de leurs problèmes avec de nouveaux outils.
Nous sommes à un tournant de notre métier. Les technologies d'attaque prennent le pas sur les technologies de protection. Le différentiel entre les hackers et ingénieurs se fait plus grand. Les systèmes sont extraordinairement vulnérables et rares sont les technologies efficaces.
Un peu, comme en médecine lors de l'apparition d'un virus. Les antibiotiques actuels se révèlent inefficaces. Alors en attendant le comblement de ce vide entre l'épée et le bouclier (avec une technologie d'Analyse comportementale par exemple), cycle immuable de la sécurité, nous avons souhaité expliquer depuis des années avec ITrust à nos clients, nos RSSI et nos RSSI, qu'il existe une autre voie complémentaire à la voie de la médecine classique. Une médecine alternative, mais complémentaire, fondée sur les meilleures pratiques et une bonne hygiène. Une sorte de "médecine chinoise" (attention sans routeur chinois « inside » ;-) qui prévient plutôt que guérir.

Alors même que la quasi-totalité des problèmes pourraient être évites simplement avec des contrôles très simples, davantage d'entreprises subissent des incidents graves liés à la cybersécurité tous les ans.
Savez-vous par exemple (mais vous devez le savoir) que la présence de mots de passe par défauts est de 98% dans les entreprises que nous auditons?

Vous n'êtes pas confrontés a des problèmes de sécurité ? C'est normal :
8 entreprises sur 10 qui subissent une intrusion ou attaque ne le savent pas
(source ITrust)

Vous avez des firewalls et des systèmes de protection et vous subissez pourtant des agressions et attaques malveillances. On nous a expliqué pendant des années qu'il fallait se protéger et le constat aujourd'hui est toujours aussi dramatique, malgré tous les outils et les budgets sécurité importants les principes de base de la sécurité ne sont pas respectés, nous sommes toujours aussi vulnérables et il est encore plus facile qu'avant pour un stagiaire de récupérer des informations confidentielles sur les réseaux ou a un étudiant coréen de récupérer la base tarifaire de votre ERP ou encore lancer une attaque ddos d'envergure sur votre infrastructure

Pour vous en convaincre :
Une anecdote qui mériterait une conférence.

Les grandes catastrophes auraient pour la plupart pu être évitées par des solutions et procédures contrôlées simples :

- ***Plate forme pétrolière BP :***
  le système de sécurité de la vanne avait été désactivé, car générant trop de faux positifs
- ***Société Générale Kerviel :***
  le trader était aussi le concepteur de l'outil de trading
- ***Fukushima :***
  Les ingénieurs étaient persuadés que la pompe de refroidissement était ouverte
- ***Le virus Stuxnet :***
  utilisait le mot de passe par défaut des équipements Siemens
- ***Drame du Hesel :***
  par manque de contrôles un trop grand nombre de spectateurs sans billets assistent au match

La plupart des incidents de sécurité auraient pu être évités simplement.
Savez-vous que la plus grande attaque informatique (Stuxnet) aurait pu être évitée en changeant le mot de passe par défaut d'un équipement siemens.
En respectant ce que l'on appelle de plus en plus aujourd'hui une bonne hygiène de sécurité : des contrôles simples, intelligents.

Ce que nous disons est confirmé par les pus grands experts ainsi que par les études.

BEST PRACTICES

« Les anti-virus ne sont plus efficaces pour répondre aux nouvelles menaces. Maintenir un bon niveau de sécurité en évitant les mots de passe par défaut et en surveillant les vulnérabilités reste lameilleure pratique de sécurité actuelle pour les PMEs. »

Hervé Schauer, *consultant en sécurité expert*

Contrôles de base

Selon une enquête menée par Verizon [1] sur les attaques réseau :
La majorité des attaques surviennent encore et toujours parce que des contrôles en place n'étaient pas implémentés de façon cohérente pour l'ensemble de l'organisation.
Beaucoup d'organisations définissent des règles et des procédures de sécurité mais négligent de les implémenter avec.

[1] « 2009 Data Breach Investigations Report », Verizon Business Risk Team

La sécurité informatique est quelque chose de simple.
Pour ne pas être malade, vous vous lavez les mains, avez une bonne hygiène , mangez équilibré ...
Vous êtes content de ne pas être gavé de médicaments tous les matins.
La SSI c'est la même chose, mais c'est un discours difficile à entendre, tant l'on nous a rabâché pendant 20 ans que les médicaments étaient la seule solution a nos maux.

Sur les dernières années notre constat, est partagé par d'autres experts : 10 failles de sécurité représentent 99% des failles et des problèmes rencontres dans tout type d'entreprise.

TOP 10 DES FAILLES DANS LES ENTREPRISES
Systèmes trop verbeux
Mots de passe faibles
Permissions et droits
Confiance interdomaine
Base de données avec mot de passe par défaut
Serveurs DNS trop verbeux
Partages de fichiers cononfidentiels
Protocoles non chiffrés ou mal configurés
Serveurs de développement ou à l'abandon
Vulnérabilités connues non corrigées

Corrigeons en priorité ces failles et le niveau de sécurité de l'entreprise augmente exponentiellement et bien mieux qu'avec n'importe quelle couteuse technologie. ITrust a développé sa solution Ikare sur la base de ces conclusions. Ikare monitor en continu les failles de sécurité d'un système d'information et propose les corrections adaptées.

Que fait la police ?

Bien souvent, le salut vient de la règlementation. C'est une fois qu'ils seront obligatoires que ces contrôles seront mis en place de manière systématique. Alors qu'en est-il ?

C'est une tendance forte, de plus en plus de recommandations ou de normes de conformité vont dans ce sens. On peut citer notamment :

- le guide d'hygiène sur la sécurité de l'ANSSI l (lien ….)
- les nouvelles contraintes liées aux données de santé, de plus en plus de recommandations
- Le top 20 SANS

LIVRE BLANC

Le Top 10 des vulnérabilités par ITrust

Bibliographie

[1] http://lexpansion.lexpress.fr/high-tech/cyberguerre-comment-les-americains-ont-pirate-l-elysee_361225.html

[2] http://www.cenzic.com/resources/reg-required/whitePapers/Ponemon2011/

[3] https://www.owasp.org/index.php/Top_10_2013-T10

[4] http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf

Rédacteurs

Lavesque Julien est directeur technique au sein d'ITrust. Il est consultant sécurité intervenant en tant qu'Auditeur, expert et formateur pour une soixantaine de clients. Ingénieur Télécom et sécurité.

Piotrowski Jean-Nicolas, PDG fondateur d'ITrust. Il est expert sécurité depuis 15 ans, ancien RSSI à la BNP Arbitrage salle de marché. Il est secrétaire général et cofondateur du cluster Digital Place.
Sur la base d'une étude cas réalisée par ***Denis Ducamp***, Consultant sécurité.

ITrust (www.itrust.fr) est une société d'expertise en sécurité depuis 2007 qui fournit son expertise et ses produits à plus de 100 clients européens.
Elle développe la solution ***IKare*** de détection de vulnérabilités (www.ikare-monitoring.com).
ITrust est lauréat des investissements d'Avenir, Projet « SVC » de sécurisation du cloud et développe une technologie de rupture concernant l'analyse comportementale.
ITrust est lauréat 2013 du prix de l'international du numérique, décerné par IEclub et Ubifrance.

ITrust
IT Security Services
55 avenue l'Occitane
BP 67303
31 670 Labège Cedex, France
Tél : +33 (0)567.346.781
Email : sales@itrust.fr
www.itrust.fr
www.ikare-monitoring.com