

Gestion des risques dans la TI compte tenu de la surveillance réseau

Livre blanc
Auteur: Dirk Paessler

Publié : Août 2008

www.fr.paessler.com
info@paessler.com

CONTENU

Sommaire	3
CLASSIFICATION DES RISQUES INFORMATIQUES SPÉCIFIQUES	4
CATÉGORIES DE RISQUES	4
Les risques techniques	4
Les risques juridiques et personnels	4
Catastrophes naturelles et causées par l'homme	5
UN CONCEPT EN 3 ÉTAPES	5
Etape 1 : Listage des risques et estimation des coûts	5
Etape 2 : Minimisation des coûts	6
Etape 3 : Planification à long terme	
GARDER UNE VUE ENSEMBLE : MINIMISATION DES RISQUES ET LE RESEAU	7
Réseaux sans fil et leurs risques spécifiques	8
GESTION DES RISQUES AVEC LES LOGICIELS DE PAESSLER	9
Résumé	10

SOMMAIRE

La vie est pleine de risques. Puisqu'il n'est pas possible d'exclure tous les risques, les entreprises prévoyantes organiseront des ressources pour minimiser les risques et pour contrôler les pertes éventuelles.

Dans la vie des affaires, le synonyme pour « gestion de risque » est en général « assurance ». Dans le domaine TI, l'accent est mis sur la réparation technique du problème apparu, la plupart du temps sans un vrai concept prévisionnel. Il est évident que cette stratégie a des graves inconvénients. Ainsi, par exemple si un problème apparaît, des ressources importantes vont être engagées pour le résoudre.

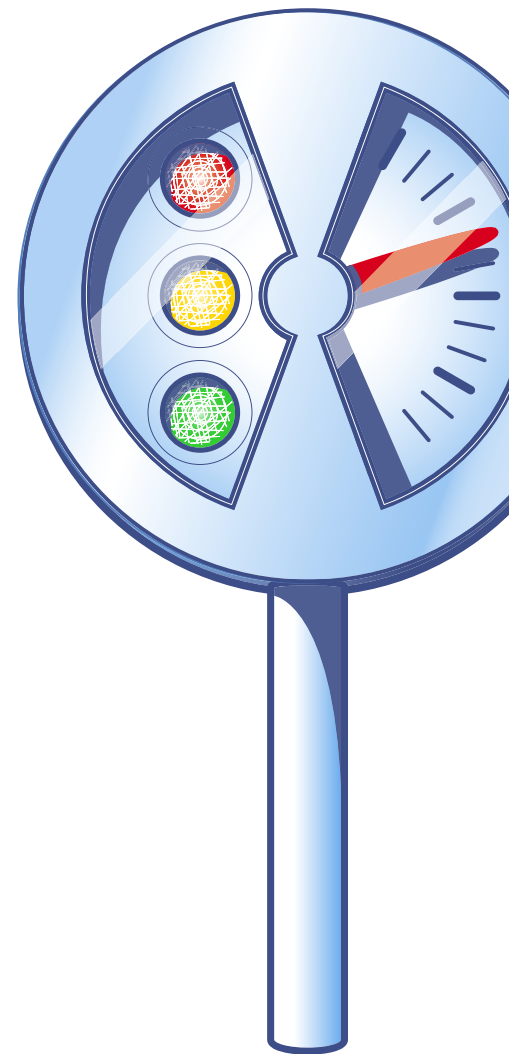
De plus, la TI a tendance à se focaliser sur deux sortes de risques : Malware (virus, chevaux de Troie) et les pertes de données (causées par Malware ou défauts du disque dur). Cela mène souvent à ignorer complètement les autres risques, qui demandent en définitive autant d'attention (voir : "IT Risk Management: A Little Bit More Is a Whole Lot Better" sur www.gartner.com).

D'un autre côté, on ne doit pas engager trop de ressources pouvant être mises en place plus raisonnablement dans d'autres domaines. Ce qui est crucial, c'est de trouver le bon équilibre et d'investir des ressources de manière réfléchie pour atteindre une minimisation des risques optimale pour des coûts minimaux.

L'importance de la surveillance réseau dans beaucoup de domaines de la gestion des risques informatiques est souvent sous-estimée et négligée. On va naturellement

investir dans des logiciels de surveillance réseau pour identifier des switchs défectueux ou des connexions surchargées. Il existe cependant beaucoup plus de potentiel, comme p.ex. la découverte des téléchargements interdits, l'optimisation du réseau complet et donc, l'accélération de tous les processus de l'entreprise ou bien aussi un facteur de sécurité additionnel en reconnaissant à temps des activités inhabituelles (Malware!). Ces facteurs sont décisifs dans un monde où des décélérations de fractions de seconde pendant la transmission des données ont souvent de graves conséquences.

Une vaste enquête très détaillée sur les risques informatiques spécifiques se trouve dans l'étude CobiT (Control Objectives for Information and related Technology) 4.1 de l' ISACA (Information Systems Audit and Control Association) sur www.isaca.org/CobiT. Cette enquête traite des risques informatiques spécifiques en tenant particulièrement compte de l'opération de réseau. Elle poursuit une approche en 3 étapes pour l'identification, l'appréciation et la planification d'une stratégie de minimisation des risques. Elle y assigne une position clef à la surveillance réseau.



Liens

Groupe Gartner:

"IT Risk Management: A Little Bit More Is a Whole Lot Better"
www.gartner.com

ISACA:

Article CobiT sur la gestion des risques
www.isaca.org/CobiT

CLASSIFICATION DES RISQUES INFORMATIQUES SPECIFIQUES

Tout d'abord, la mauvaise nouvelle: les risques ne peuvent pas être exclus complètement. Le but de la gestion des risques est d'une part d'identifier les problèmes qui peuvent (et doivent) être minimisés et d'autre part de plafonner les coûts à un niveau étant acceptable pour une entreprise. Mais cela comporte toujours un risque résiduel inévitable pour l'entreprise.

Des petites et moyennes entreprises (PME) peuvent être confrontées à des risques peu probables mais pouvant menacer leur existence et qui doivent être acceptés, car l'effort pour éviter ces risques ne pourrait pas être supporté par l'entreprise.

Ce sont malheureusement surtout les PME du domaine TI qui réagissent seulement quand leur sécurité est menacée et donc sans une vraie gestion prévisionnelle des risques : des virus informatiques menacent, puis la TI installe un logiciel anti-virus ; des chevaux de Troie menacent, la TI installe un pare-feu, etc.

Cette procédure implique surtout deux problèmes :

- Premièrement, elle est myope : Elle considère seulement une partie du risque total – normalement les risques pouvant être résolus techniquement.
- Deuxièmement, elle est peu systématique et réactive : Elle mène à une accumulation de

matériels et de logiciels, chacun ayant été commandé à cause d'un seul problème, sans une gestion centrale ou un concept constant. Un département informatique qui joue en permanence au « pompier » ne peut jamais avoir un vrai succès. Dans ce cas, il faut reculer d'un pas et développer un concept de risque.

CATÉGORIES DE RISQUE

La TI est confronté pour l'essentiel à trois catégories de risques :

Les risques techniques

Les risques techniques sont les centres d'intérêts traditionnels de la TI allant des défaillances causées par les virus jusqu'aux cas plus exotiques, comme p.ex. les attaques « Denial-of-Service » ou les dénommés « War Walkers ». Des « War Walkers » désignent des pirates (hackers) qui infiltrent le réseau sans fil à partir de l'extérieur de l'entreprise.

La plupart de mesures contre ces problèmes sont également de nature technique, en effet, des directives d'entreprise strictes dans ce domaine ont une importance cruciale. L'installation de pare-feux et de systèmes anti-virus sur des outils portables est une mesure manifestement évidente. Une autre directive judicieuse serait d'interdire aux collaborateurs d'installer de nœud WiFi incontrôlés (et souvent non protégés).

Une solution performante pour la surveillance réseau, comme p.ex. PRTG Network Monitor de Paessler AG, peut reconnaître à temps des activités inhabituelles et ainsi

suspectes dans le réseau et peut aussi, en plus d'une simple alerte, identifier l'expéditeur.

Les risques juridiques et personnels

Il est ici question de la préparation des réclamations juridiques éventuelles, comme p.ex. l'archivage du trafic email. Mais des collaborateurs faisant des téléchargements illégaux via leur accès internet de l'entreprise ou se livrant à de l'espionnage ou du sabotage, jouent également un rôle important.

Ces dangers sont plus difficiles à gérer car la technique ne peut pas apporter des solutions précises. Des directives strictes et un bon management du personnel sont les clés pour la minimisation de ces risques.

Des supérieurs devraient être suffisamment entraînés en management du personnel. L'idée qu'un employé ne sera un bon supérieur qu'à l'aide d'une promotion est une erreur répandue.

Ici aussi, une surveillance réseau professionnelle utilisée correctement peut minimiser quelques risques potentiels. Ainsi par exemple, PRTG Network Monitor offre à l'aide d'une multitude de sondes WMI la surveillance des serveurs Exchange, fournit en permanence des données Live en fonction du type et du volume du trafic réseau, et alerte activement en cas de caractères frappants et de changements.

Catastrophes naturelles et causées par l'homme

Des débordements, des incendies ou des dégâts causés par la tempête ne sont pas très vraisemblables, mais quand ils ont lieu, ils ont cependant des conséquences d'autant plus dramatiques.

Trouver des stratégies adéquates pour ces risques, c'est une des tâches les plus difficiles de la gestion des risques.

De nombreuses stratégies sont offertes avec des prix différents et des étapes de protection variées. Toutes ces stratégies doivent être jugées conjointement avec la situation totale de l'entreprise.

Avant tout, la gestion des catastrophes doit être considérée avec du bon sens.

Dans le monde connecté d'aujourd'hui, même de relatives petites entreprises peuvent installer leur centre de données dans des équipements modernes et sûrs, loin de régions menacées de catastrophes (peut-être conjointement avec d'autres entreprises). Des fonctionnalités TI existantes peuvent être également délocalisées sous forme de SaaS (Software-as-a-Service) aux prestataires de service garantissant un niveau de sécurité nettement plus haut que celui que l'entreprise peut atteindre dans son propre local à des coûts défendables.

En minimisant ces risques, une surveillance réseau fiable comme p.ex. PRTG, joue parallèlement un rôle qui ne doit pas être sous-estimé. Peu importe si l'entreprise délocalise son centre informatique à son propre compte ou comme service à un prestataire : Une disponibilité

permanente et une performance maximale au transfert de données sont des exigences essentielles pour un centre informatique externe et seulement une surveillance permanente et fiable peut le garantir.

UN CONCEPT EN 3 ÉTAPES

Même si de nombreuses petites entreprises et départements TI négligent la planification de leur minimisation de risques, trop de planification n'est pas raisonnable non plus. Surtout les PME mais également des entreprises plus grandes peuvent planifier aisément leur gestion des risques de façon plus étroite et plus souple.

Etape 1 : Listage des risques et estimation des coûts

La première étape d'une gestion des risques stratégiques est d'identifier les risques principaux des trois catégories de risque mentionnées ci-dessus.

Il y a différentes listes de risques standard, l'enquête CobiT en contient une des plus complètes. Toutefois, celles-ci sont souvent trop vastes et globales pour les centres d'intérêts d'un département TI ou d'une plus petite entreprise TI.

Chaque projet contient une série de risques propres spécifiques, y compris le danger que la tâche ne soit jamais terminée ou déficiente ou que le budget et le calendrier soient dépassés.

Le pur établissement d'une liste de tous les risques est en général

relativement facile. Mais en revanche, l'appréciation de ces risques en vue des coûts potentiels et des conséquences pour l'entreprise est nettement plus difficile. Alors que les listes de risques peuvent être utilisées en général universellement, les coûts étant causés par ces risques peuvent varier d'une entreprise à l'autre.

Par exemple pour des entreprises financières, les plus petits ralentissements peuvent avoir de graves conséquences lors d'un transfert de transaction, alors que les entreprises de l'industrie ont une plus grande tolérance, mais elles sont en revanche hautement dépendantes de la performance de leur système ERP. Cela rend compliqué une estimation précise des coûts des risques individuels pour l'entreprise correspondante.

Le responsable de la gestion des risques essaiera de recueillir un maximum d'informations sur non seulement de la part des décideurs de son entreprise mais aussi de la part des organisations du secteur ou des collègues d'autres entreprises de son secteur.

L'estimation des coûts ne doit pas être précise. Tout d'abord il est important d'avoir une estimation générale. Celle-ci est la base pour la décision portant sur l'effort qui doit être investi pour une minimisation des risques. En outre, il faut cibler ce qui doit être planifié pour la protection de l'entreprise des dangers standard, comme p.ex. des virus ou chevaux de Troie.

Les questions les plus importantes pour le concepteur sont :

Quelle somme doit être planifiée pour les risques standard par rapport à d'autres risques ?

Quand les dépenses dépassent-elles le cadre coût-utilité?

Les réponses à ces questions fondamentales dépendent en dernier lieu aussi des coûts pouvant être causés par des risques TI en cas de dommage.

En outre, on doit prendre en compte la probabilité que le dommage entraîne. Ainsi par exemple, les virus sont des problèmes permanents quoique le seul virus ne cause en général pas de grands dommages et puisse être éliminé avec relativement peu d'efforts. Des catastrophes sont de loin beaucoup moins vraisemblables, mais lorsqu'elles apparaissent, elles peuvent ruiner complètement l'entreprise.

Etape 2 : Minimisation des coûts

Une première estimation des coûts ne doit pas contenir de chiffres exacts – il n'est pas nécessaire de demander d'ores et déjà un devis. Des estimations générales à l'aide d'une recherche internet ou à l'aide des valeurs empiriques sont entièrement suffisantes. Il est important de considérer aussi le temps de travail nécessité par les collaborateurs engagés, en plus des fonds à dépenser. Une estimation des coûts est très facile, tant que la minimisation des risques peut être limitée à l'achat et l'installation de matériels et logiciels. De plus et particulièrement en cas de catastrophe, il existe des stratégies variées avec des coûts et une efficacité différents.

On doit considérer différents facteurs en fonction de la stratégie décidée comme la plus appropriée pour sa propre entreprise :

- Seuil de tolérance d'une longue durée d'immobilisation
- Ressources disponibles pour la solution du problème
- Potentiel de l'entreprise de survivre à une plus grande catastrophe (tolérance au risque)

Une petite entreprise qui ne peut pas survivre à une catastrophe gaspillerait de l'argent pour l'établissement d'un centre informatique externe pour la sauvegarde et la récupération de données (DR – data recovery). Si l'entreprise n'a les moyens que pour la sauvegarde des données sur un porteur de données, cette sauvegarde sera la solution DR de l'entreprise, et ceci qu'elle réalise les vrais exigences DR de l'entreprise ou pas. Dans ce cas, des alternatives comme des prestataires SaaS peuvent être une option intéressante.

Pendant la planification de la minimisation des risques il peut s'avérer que les coûts de la minimisation peuvent dépasser les dommages présumés. Dans ce cas, on doit faire abstraction d'une minimisation des risques.

En déterminant la stratégie de la minimisation des risques, la direction de l'entreprise doit également considérer la tolérance de risque de l'entreprise.

Etape 3 : Planification à long terme

La minimisation des risques est un processus permanent. Avant tout la pénurie de ressources libres requiert une planification à long terme. Les risques se transforment avec le temps et donc, des stratégies doivent être contrôlées en permanence et si nécessaire, adaptées.

Le danger des virus est un risque constant, mais en revanche, les seuls virus changent sans arrêt. C'est pourquoi une entreprise, si expérimentée soit-elle dans le domaine de la protection de virus, doit cependant être sous une vigilance constante pour pouvoir réagir aux nouveaux virus.

Des nouveaux dangers peuvent apparaître à tout moment, comme par exemple par des réseaux sans fil et War Walkers, et notamment l'expansion des entreprises dans de nouveaux marchés et de nouvelles branches commerciales augmentent de manière significative le risque principal.

GARDER UNE VUE ENSEMBLE : MINIMISATION DES RISQUES ET LE RESEAU

Lors de la planification de la gestion des risques accompagnée de la planification TI, on doit toujours garder à l'œil la fonctionnalité du réseau complet.

A côté des coûts, il faut considérer aussi d'autres facteurs lors de réflexions sur la minimisation de risques, comme p.ex. la question de savoir si des mesures internes doivent être prises ou si une externalisation est plus raisonnable.

Cette décision est souvent prise en raison des coûts relatifs, en raison de la disponibilité ou d'un savoir-faire spécifique ou pour des raisons de politique d'entreprise. Mais c'est avant tout le scénario de risque total qui peut être fondamentalement influencé.

Des risques comme la sécurité ou la récupération de données peuvent être transmis au prestataire de services. Cependant, l'entreprise court ainsi de nouveaux risques. Le prestataire de services ne peut probablement pas respecter des SLA (Service Level Agreements / Accords sur la qualité de service) ou des SLA arrangés ne correspondent pas aux vraies exigences de l'entreprise. Le transfert de risques accompagné d'une baisse de coûts exigera de nouveaux investissements dans le domaine du contrôle de la prestation.

Tout cela nécessite une planification réfléchie, accompagnée d'une

prise de décision prudente, mais il peut finalement mener à une minimisation de risques significative avec des coûts justifiables.

La surveillance réseau est un autre outil important pour la minimisation des risques qui est utilisé trop peu souvent. Cette technologie est souvent utilisée seulement dans le contexte de la défaillance de composants réseau et de lignes de données surchargées. C'est elle qui offre aussi de nombreuses possibilités pouvant être utilisées dans les différents domaines de la gestion de risques pour un soutien plus ou moins direct.

L'un des risques principaux est le ralentissement pendant le transfert de données causé par une augmentation du trafic réseau.

On sait que la VoIP (la voix sur réseau IP) réagit de façon très sensible à ces ralentissements de sorte que le lancement de VoIP est souvent accompagné d'une priorité plus haute pour les paquets VoIP pour qu'ils ne soient pas altérés.

Mais d'autres applications peuvent réagir aussi sensiblement aux ralentissements pendant le transfert de données. C'est ainsi qu'un ralentissement pendant le transfert de données peut causer des dommages allant jusqu'à des pertes boursières pour des entreprises telles que des compagnies aériennes ou des prestataires de service financiers.

Dans les usines modernes et hautement automatisées, des ralentissements pendant le transfert de données peuvent contrarier des installations complètes de production et mener à des pertes de production. La perte de commandes passées automatiquement ou de données de délais de livraison pour

des productions commandées à base de JIT (just-in-time ; juste à temps) peut avoir de conséquences catastrophiques. Une surveillance réseau professionnelle peut donc garantir la ROI (Return on investment ; Retour sur Investissement) de beaucoup d'entreprises fabricantes du seul fait que des données importantes atteignent leur but sans retard.

Une surveillance conséquente peut aussi aider à identifier une augmentation données et leurs causes. Le monde des affaires moderne devient de plus en plus mobile et aujourd'hui, ce ne sont pas seulement les managers qui utilisent des ordinateurs portables ou des PDA (Personal Digital Assistant). De plus en plus de collaborateurs utilisent des outils mobiles hors des réseaux d'entreprise protégés et augmentent ainsi le risque que des virus, des chevaux à Troie etc. passent à travers les pare-feux des entreprises.

Le premier avertissement à de tels dangers – lorsqu'un ordinateur infecté envoie en masse des Spam ou lance des attaques Denial-of-Service, ou quand un virus s'étend sur le réseau – caracole en tête dans le trafic réseau qui sont découverts par des outils de surveillance. Ceux-ci sont souvent les premiers éléments qui identifient les causes des problèmes de sorte qu'ils peuvent les éliminer.

Réseaux sans fil et leurs risques spécifiques

Des réseaux sans fil sont de plus en plus utilisés et sont accompagnés des risques différents :

La TI perd une grande partie du contrôle sur les outils qui sont reliés au réseau. Cela implique des risques allant d'une incompatibilité entre des applications et des outils connectés jusqu'aux accès au réseau par des visiteurs et des personnes non autorisées.

Le réseau va souvent au-delà du site de l'entreprise et ainsi, il est attaquant pour des War Walker qui se trouvent près des parkings et des trottoirs qui jouxtent les murs de l'entreprise et ont accès au réseau d'entreprise et probablement aux applications et données internes.

On sait que des modems sans fil peuvent être connectés très facilement à un réseau. Des administrateurs de réseau découvrent souvent des réseaux sans fil non autorisés qui apparaissent subitement dans des bureaux d'entreprise après que des employés ont connectés des modems sans fil au réseau dans leur bureau. Souvent, ces employés ne font pas l'effort d'activer les contrôles d'accès de ce modem et ainsi, ils ouvrent une brèche pour des intrus qui peuvent ainsi passer à travers le pare-feu et pénétrer dans le réseau d'entreprise ou introduire des logiciels espions.

Une surveillance réseau professionnelle peut aussi dans ce cas aider la TI à découvrir et à minimiser les risques potentiels découlant nécessairement de l'utilisation des réseaux sans fil et elle peut donc

ainsi contrôler des environnements réseau sans fil.

Une surveillance sans faille du volume du trafic réseau est particulièrement important aujourd'hui parce qu'il y a eu un changement essentiel de la sorte et de la quantité des données professionnelles échangées. Les fichiers texte qui constituaient jusque récemment une grande partie du volume de données professionnelles, sont entre-temps progressivement remplacés par des fichiers graphiques et de données audio et vidéo. Par conséquent, un réseau ayant été conçu pour le transfert des données de texte, atteint rapidement à ses limites. Il est difficile de faire la distinction entre un envoi de données légales et commerciales et une conversation privée ou même des contenus discriminants.

Les pages comme par exemple YouTube sont souvent des expéditeurs d'un trafic important, en effet les données envoyées légitimement deviennent de plus en plus vastes. Ainsi de nombreuses entreprises remplacent par exemple des voyages d'affaires par des conférences vidéo et par téléphone fréquemment dans des salles de conférences spécifiques, mais souvent aussi à partir de postes de travail individuels. L'entreprise fait ainsi beaucoup d'économies sur les voyages, augmente sa productivité et diminue en même temps la charge de travail de ses employés par la suppression du temps de voyage et elle protège aussi l'environnement.

L'augmentation rapide du volume de données ainsi que l'augmentation continue du coût du carburant accentuent le risque de goulots d'étranglement et de baisses de performance dans le

La société Paessler AG

La société Paessler AG dont le siège se trouve à Nuremberg (Allemagne) développe des logiciels dans les domaines de la surveillance réseau et de l'analyse de serveurs Web depuis 1997. Les produits de Paessler sont utilisés dans le monde entier par plus de 150.000 administrateurs de système, opérateurs de site web, fournisseurs d'accès Internet et autres spécialistes de l'informatique. Des versions gratuites et de démonstration sont disponibles en ligne sur le site www.fr.paessler.com.

réseau. Une solution de surveillance réseau performante comme par exemple PRTG Network Monitor de Paessler peut, en plus de la surveillance en temps réel, documenter et analyser l'augmentation du volume de données par des évaluations de données à long terme. Ainsi, elle peut minimiser ce risque d'une part en identifiant des expéditeurs à forte activité et d'autre part en permettant une planification selon les besoins lors de l'expansion du réseau.

GESTION DES RISQUES AVEC LES LOGICIELS DE PAESSLER

La Paessler AG (Paessler SA (Société Anonyme)) s'est spécialisée dans les logiciels de surveillance réseau et avec PRTG Network Monitor, elle offre une vaste solution pour la surveillance de la disponibilité et de la bande passante pour des réseaux de toutes dimensions. PRTG Network Monitor s'illustre par une installation et utilisation faciles, une haute performance et un vaste panel de fonctionnalités pratiques.

Ainsi, PRTG Network Monitor offre aux administrateurs TI un contrôle permanent de leur réseau complet en temps réel ainsi que la possibilité d'identifier les tendances d'utilisation à long terme à l'aide de données historiques. L'additif « sonde NetFlow » permet l'évaluation de protocoles NetFlow et par conséquent une surveillance générale des matériels Cisco étant compatible avec ce protocole (www.fr.paessler.com/prtg7).

En complément à PRTG, Paessler offre SNMP Helper pour permettre de collectionner et d'analyser un nombre illimité d'informations sur les systèmes Windows à l'aide de WMI (www.fr.paessler.com/snmphelper).

Webserver Stress Tool est un logiciel de test pour les serveurs HTTP (serveurs Web) qui identifie les problèmes de performance latents de serveurs Web ou bien des applications Web qui se manifestent en cas de grande charge. A travers une simulation avec des centaines ou des milliers d'utilisateurs envoyant simultanément des demandes HTTP à un serveur, Webserver Stress Tool teste le comportement de serveurs Web en cas de charge normale et extraordinaire. (www.fr.paessler.com/webstress).

Toutes les solutions Paessler sont disponibles en diverses versions, comme la version freeware avec une performance limitée et comme la version d'évaluation de 30 jours.

RÉSUMÉ

Il n'y a pas de garantie absolue. La vie est pleine de risques et une certaine partie de risques doit être acceptée par chaque entreprise. La gestion de risques ne peut pas garantir l'élimination totale de risques – même le scénario le plus sûr sera sans cesse confronté à des problèmes.

Le but d'une gestion de risques stratégique doit être de réduire le danger à un niveau acceptable qui d'une part soit financier et d'autre part ne menace plus l'existence de l'entreprise. Dès que la TI a atteint ces conditions, leur gestion de risques est couronnée de succès.



Logiciels Paessler

PRTG Network Monitor
Surveillance de la disponibilité et de la bande passante dans des réseaux
www.fr.paessler.com/prtg

SNMP Helper
Surveillance des paramètres système Windows
www.fr.paessler.com/snmphelper

WEBSERVER STRESS TOOL
Test de performance, de charge et de stress de serveur Web
www.fr.paessler.com/webstres

 **PAESSLER®**
the network monitoring company

Paessler AG • Burgschmietstraße 10
90419 Nuremberg • Allemagne
www.fr.paessler.com • info@paessler.com