Deloitte General Services
560, rue de Neudorf
L-2220 Luxembourg
P.O. Box 1173
L-1011 Luxembourg

Tel: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu

Press release

Loren Motiani
Marketing & Communications
Tel: +352 451 452 434
Email: lupress@deloitte.lu

Deloitte's 10 tips for better cyber security

Addressing the increasing threat of cyber-attacks, several international Deloitte cyber experts have analysed the current situation in the market and presented 10 key recommendations. The main aim of the 10 steps is to ensure that sufficient procedures are in place to react to cyber-attacks, from technical, business and organisational standpoints to frequently testing the ability of the systems to detect intrusions and withstand an attack.

The 10 recommendations for combatting unauthorised access to corporate networks and data range from the basic to the advanced:

1) **Focus on what matters:** identify and document the business-critical functions and information assets that must be safeguarded against cyber-attacks

2) **Get real about risk:** no matter how strong the current security measures, cyber criminals likely know how to circumvent them. That is why a risk-based approach to cyber security is needed, one that prioritises risks based on their likelihood and impact, in order to effectively manage cyber risk exposure

3) **Know your friends:** in a recent Deloitte survey of technology, media, and telecom companies, 92% of participants felt an average or high level of threat from third parties. To help combat this, extended relationships should be inventoried: supply chain, outsourcing, clients, vendors, contractors, etc. Anyone who has access to the IT infrastructure needs to be included and assurances from these parties that they are vigilant in addressing cyber security need to be affirmed

4) **Become a detective:** develop capabilities for detecting threats to business-critical functions, information assets and operational continuity. By centrally monitoring systems, cyber threats can be detected in real time, enabling a quick response to mitigate negative impacts

5) **Draw up emergency plans:** when it comes to cyber attacks, prevention is only half the battle. Even the best systems and most vigilant organisations can be compromised. That is why procedures to react to cyber attacks need to be established, from legal, technical, business, organisational and branding standpoints

6) **Crash your own gates:** cyber simulations can help test the effectiveness of emergency responses and the ability of systems to detect intrusions and withstand attacks. This enables the improvement of resiliency plans and defensive strategies to recover quickly

7) **Protect what is vulnerable:** cyber criminals increasingly evade current security controls to target vulnerable applications. To protect business-critical systems, make sure to apply timely patches and software updates to the most exposed assets

8) **Get smart:** enhance the organisation's ability to proactively detect and mitigate imminent and emerging cyber threats by leveraging the knowledge of industry associations, as well as

commercial and open source intelligence sources. Whether the skills are built in-house or outsource, the key is to establish proactive cyber threat intelligence capabilities

9) **Jealously guard your reputation:** companies that suffer a cyber-attack face more than financial loss. They also risk brand damage and the loss of public confidence. To protect its reputation, one needs to know who is talking about the brand and what they are saying. By consistently monitoring its brand on the Internet, trademark, copyright and other intellectual property infringement can often be avoided. More significantly, by improving cyber security stance, corporate assets and sensitive customer and employee data from the outset can be protected

10) **Foster cyber awareness**: the weakest link in cyber security is not technology; it is people. Social engineering attacks that use targeted phishing emails or other techniques often hoodwink users into revealing confidential information or trick them into downloading malware. This makes it easier for cyber criminals to penetrate networks, without even resorting to more traditional hacking methods. Employees need to be educated to make sure they are aware of these risks and threats

According to Roland Bastin, partner at Deloitte Luxembourg: "*Cyber security no longer exclusively addresses CIOs and IT departments. The threat has become so pervasive, the points of illegal entry so numerous and the implications of a breach so serious that every member of the organisation has a stake and a role in protecting the company from cyber-attacks.*"

Prior to drawing up the list, Deloitte was named a global leader in cyber security consulting in the *Cyber Security Consulting 2013* report released by Kennedy Consulting Research and Advisory, a leading analyst firm.

It is not the first time that Deloitte's risk services are rewarded for their expertise in cyber security. In recent months, many analysts have praised the governance, risk and compliance services of the company in the fields of risk management consulting, security consulting; information security consulting, and more. What the Kennedy report emphasises is the effectiveness of the integrated, full-spectrum approach chosen by the company, which led to the most comprehensive set of capabilities on the cyber security market.

"*Deloitte brings a strong value proposition to cyber security consulting by melding its industry expertise, its 'one approach, one model,' cyber security-specific investments, and C-suite communication capabilities*" the Kennedy report notes.

Les 10 commandements de Deloitte pour une cybersécurité renforcée

Face à la menace croissante des cyberattaques, plusieurs experts internationaux de la communication numérique de Deloitte ont analysé la situation actuelle sur le marché et formulé dix recommandations-clés. L'objectif premier de ces dix mesures de précaution consiste à mettre en place les procédures suffisantes, d'un point de vue technique, commercial et organisationnel, pour réagir aux cyberattaques, afin de tester régulièrement la capacité des systèmes à détecter les intrusions et à repousser les attaques.

Ces dix commandements de la lutte contre l'accès non autorisé aux réseaux d'entreprises et aux données vont du plus élémentaire au plus pointu :

1) **Allez à l'essentiel :** identifiez et documentez les fonctions critiques dans l'entreprise et les données qui doivent être protégées des cyberattaques.

2) **Faites preuve de réalisme en matière de risque :** quelle que soit la solidité de vos mesures de sécurité actuelles, les cybercriminels sauront comment les contourner. C'est pourquoi une approche fondée sur le risque s'impose, de manière à pouvoir hiérarchiser les risques en fonction de leur probabilité et de leur impact, dans le cadre d'une gestion efficace de l'exposition aux risques cybernétiques.

3) **Sachez reconnaître vos amis :** dans le cadre d'une récente étude de Deloitte consacrée aux sociétés des secteurs de la technologie, des médias et des télécommunications, 92% des répondants ont déclaré ressentir un niveau de menace moyen à élevé vis-à-vis des tiers. Pour remédier à cette menace, il est conseillé de dresser l'inventaire de ses relations au sens large : chaîne d'approvisionnement, externalisation, clients, fournisseurs, contractants, etc. Tout individu ayant accès à l'infrastructure IT doit être identifié et pouvoir montrer patte blanche en termes de gestion de la sécurité informatique.

4) **Revêtez votre costume de détective :** développez vos capacités à détecter les menaces qui planent sur les fonctions critiques de votre entreprise, les données et la continuité des opérations. En contrôlant les systèmes de manière centrale, vous pourrez détecter les menaces en temps réel, et donc y répondre rapidement afin de limiter leurs effets négatifs.

5) **Etablissez des plans d'urgence :** face aux cyberattaques, la prévention ne constitue que la moitié de la bataille. Même les meilleurs systèmes et les organisations les plus vigilantes peuvent être pris en défaut. C'est pourquoi il est nécessaire d'établir des procédures de réaction aux cyberattaques, tant d'un point de vue légal, technique, commercial, organisationnel qu'au niveau de la marque.

6) **Testez vous-même la solidité de vos protections :** les simulations vous permettront d'éprouver l'efficacité des réponses en cas d'urgence et la capacité de vos systèmes à détecter les intrusions et à repousser les attaques. Ainsi, vous pourrez encore améliorer vos plans de résilience et vos stratégies de défense afin de recouvrer rapidement toutes vos capacités.

7) **Protégez ce qui est vulnérable :** les cybercriminels se montrent de plus en plus habiles pour échapper aux contrôles de sécurité existants et ciblent les applications vulnérables. Afin de protéger les systèmes critiques de votre entreprise, veillez à appliquer à temps les correctifs et les mises à jour de logiciels pour sécuriser vos actifs les plus exposés.

8) **Soyez malin :** optimisez la capacité de l'organisation à se montrer proactive dans la détection et l'atténuation des menaces cybernétiques imminentes et émergentes en exploitant le savoir des associations sectorielles, ainsi que les sources d'intelligence commerciales et « open source ». Que le développement des compétences se fasse en interne ou qu'il soit externalisé, la clé est d'établir des capacités d'intelligence proactives face aux menaces cybernétiques.

9) **Protégez jalousement votre réputation :** les sociétés victimes d'une cyberattaque sont exposées à bien plus que des pertes financières. Un risque d'atteinte à la marque et de perte de confiance du public existe également. Pour préserver votre réputation, vous devez savoir qui parle de votre marque et ce qu'il se dit. En assurant un contrôle permanent de la marque sur Internet, il est souvent possible d'éviter les violations de marque commerciale, des droits d'auteur et de la propriété intellectuelle. En outre, en améliorant la sécurité cybernétique, vous protégerez dès le début les actifs de l'entreprise et les données sensibles sur les clients et les employés.

10) **Encouragez la « cyber awareness » :** le maillon faible de la sécurité des réseaux de communication numériques n'est pas la technologie, mais bien ses utilisateurs. Les attaques

d'ingénierie sociale qui utilisent des e-mails de « phishing » ciblés et autres techniques s'évertuent souvent à duper les utilisateurs pour qu'ils révèlent des informations confidentielles ou téléchargent des logiciels malveillants. Ainsi, il est plus aisé pour les criminels informatiques de pénétrer les réseaux, même sans avoir à faire appel aux méthodes de « hacking » traditionnelles. Les employés doivent donc être formés et sensibilisés à ces risques et menaces.

Roland Bastin, partner chez Deloitte Luxembourg : « *La cybersécurité n'est plus exclusivement l'affaire des CIO et des départements IT. La menace est devenue à ce point omniprésente, les points d'entrée illégaux à ce point nombreux et les implications d'une violation à ce point importantes qu'il est de la responsabilité de chaque membre d'une organisation d'assurer la protection de la société face aux cyberattaques.* »

Préalablement à l'établissement de ces « dix commandements », Deloitte a été désigné leader mondial du conseil en cybersécurité dans le cadre du rapport *Cyber Security Consulting 2013* publié par le célèbre cabinet d'analyse Kennedy Consulting Research and Advisory.

Cette récompense n'est cependant pas une première pour les services Risque de Deloitte. De nombreux analystes ont récemment fait l'éloge des services Gouvernance, Risque et Conformité de la société dans les domaines du conseil en gestion du risque, conseil en sécurité, conseil en sécurité des informations, et bien d'autres. Le rapport Kennedy met d'ailleurs en évidence l'efficacité de l'approche intégrée et exhaustive choisie par le cabinet Deloitte, qui fait de l'éventail de compétence de la firme le plus complet du marché de la sécurité cybernétique.

Selon le rapport, « *Deloitte apporte une proposition de valeur de poids dans le conseil en sécurité cybernétique, en combinant son savoir-faire sectoriel, sa stratégie « une approche, un modèle », des investissements spécifiques dans la cybersécurité et les capacités de communication de ses cadres* ».

Deloitte: 10 Tipps für eine bessere Cyber-Sicherheit

Damit Unternehmen angemessen auf die wachsende Bedrohung durch Cyber-Attacken reagieren können, haben internationale Cyber-Experten von Deloitte auf Basis der aktuellen Marktsituation 10 Empfehlungen zusammengestellt. Durch diese 10 Schritte soll sichergestellt werden, dass angemessene Verfahren und Maßnahmen vorhanden, um auf Cyber-Attacken reagieren zu können – vom technischen, geschäftlichen und organisatorischen Gesichtspunkten bis hin zu regelmäßigen Systemtests, um Attacken frühzeitig zu erkennen und abzuwehren.

Die 10 Empfehlungen zur Abwehr von unautorisierten Zugriffen auf Unternehmensnetzwerke und -daten reichen von allgemeinen Tipps bis hin zu erweiterten Maßnahmen:

1) **Konzentrieren Sie sich auf das Wesentliche:** Identifizieren und dokumentieren Sie die geschäftskritischen Funktionen und Informationen, die vor Cyber-Attacken geschützt werden müssen.

2) **Seien Sie sich der Risiken bewusst:** Egal, wie intensiv die aktuellen Sicherheitsmaßnahmen sind, Cyber-Kriminelle wissen, wie sie diese umgehen können. Deshalb ist ein risikobasierter Ansatz bezüglich der Cyber-Sicherheit erforderlich, denn dieser priorisiert Risiken auf Basis der Wahrscheinlichkeit des Auftretens und der sich daraus ergebenden Auswirkungen, wodurch Cyber-Sicherheit effektiv umgesetzt werden kann.

3) **Kennen Sie Ihre Freunde:** In einer kürzlich durchgeführten Umfrage von Deloitte bei Technologie-, Medien- und Telekommunikationsunternehmen gaben 92 % der Teilnehmer an, dass sie sich von Dritten durchschnittlich bis stark bedroht fühlen. Um dem entgegenzuwirken, sollten die Beziehungen zu Ihren Geschäftspartnern genauer unter die Lupe genommen werden: Lieferkette, Outsourcing, Kunden, Hersteller, Auftragnehmer usw. Jeder, der Zugriff auf die IT-Infrastruktur hat, ist hiervon betroffen. Diese Parteien müssen versichern bzw. bekräftigen, dass sie selbst im Rahmen der Cyber-Sicherheit wachsam agieren.

4) **Entwickeln Sie detektivische Fähigkeiten:** Entwickeln Sie Fähigkeiten zum Erkennen von Attacken, die geschäftskritische Funktionen, Informationen und die betrieblichen Abläufe bedrohen. Durch das zentrale Überwachen von Systemen können Cyber-Bedrohungen in Echtzeit erkannt werden, was eine schnelle Reaktion ermöglicht und negative Auswirkungen verhindert.

5) **Erstellen Sie Notfallpläne:** Bei Cyber-Attacken ist Vorsorge nur die halbe Miete. Selbst die besten Systeme und wachsamsten Organisationen sind vor Angriffen nicht sicher. Deshalb müssen Verfahren zum Reagieren auf Cyber-Attacken eingerichtet werden – und zwar vom rechtlichen, technischen, geschäftlichen, organisatorischen und vom Markenstandpunkt aus.

6) **Simulieren Sie Angriffe:** Cyber-Simulationen können dabei helfen, die Effektivität der Notfallreaktionen sowie die Fähigkeit der Systeme zu testen, Attacken zu erkennen und standzuhalten. Dadurch können Ausfallpläne und Verteidigungsstrategien verbessert werden, um eine schnelle Wiederherstellung der Systeme zu ermöglichen.

7) **Schützen Sie, was anfällig ist:** Cyber-Kriminellen gelingt es immer häufiger, Sicherheitskontrollen zu umgehen, um anfällige Anwendungen zu attackieren. Um geschäftskritische Systeme zu schützen, sollten Sie rechtzeitig Patches und Software-Updates für die am meisten gefährdeten Ressourcen aufspielen.

11) **Seien Sie klug:** Verbessern Sie die Fähigkeit des Unternehmens, bevorstehende und neu auftauchende Cyber-Bedrohungen proaktiv zu erkennen und die Folgen zu mildern, indem Sie die Kenntnisse von Industrieverbänden sowie die Angebote von kommerziellen und Open Source-Anbietern nutzen. Ob dieses Wissen intern erworben oder extern herangezogen wird, ist weniger entscheidend. Wichtig ist, dass proaktive Abwehrmaßnahmen gegen Cyber-Bedrohungen ergriffen werden.

12) **Seien Sie strengstens auf Ihren guten Ruf bedacht:** Für Unternehmen, die Cyber-Attacken ausgesetzt sind, geht es um mehr als finanzielle Verluste. Sie riskieren zudem, dass ihre Marken geschädigt werden, sowie einen Vertrauensverlust in der Öffentlichkeit. Um Ihren Ruf zu schützen, müssen Sie wissen, wer über Ihre Marke spricht und was darüber gesagt wird.

Durch permanentes Überwachen der eigenen Marke im Internet kann der Verstoß gegen Markenrechte, Urheberrechte und andere geistige Eigentumsrechte oft vermieden werden. Noch wichtiger ist es, durch Verbessern der Cyber-Sicherheit Unternehmensressourcen und vertrauliche Kunden- und Mitarbeiterdaten von Beginn an zu schützen.

13) **Fördern des Sicherheitsbewusstseins bezüglich Cyber-Attacken**: Das schwächste Glied bei der Cyber-Sicherheit ist nicht die Technologie, es sind die Menschen. Social-Engineering-Attacken, die gezielt Phishing-E-Mails oder andere Techniken einsetzen, bringen Anwender oft dazu, ihre persönlichen Daten preiszugeben oder Malware herunterzuladen. Dadurch können Cyber-Kriminelle einfacher Netzwerke angreifen, ohne auf traditionelle Hacking-Methoden zurückgreifen zu müssen. Die Mitarbeiter der Unternehmen müssen geschult werden, damit sichergestellt wird, dass sie diese Risiken und Bedrohungen kennen.

Dies sagt Roland Bastin, Partner bei Deloitte Luxemburg, dazu: „*Cyber-Sicherheit richtet sich nicht mehr nur exklusiv an CIOs und IT-Abteilungen. Die Bedrohung ist so allgegenwärtig, die illegalen Eintrittspunkte sind so zahlreich und die Auswirkungen eines Verstoßes so ernsthaft geworden, dass jeder Mitarbeiter eines Unternehmens beim Schutz desselben vor Cyber-Attacken seinen Anteil beizutragen hat.*“

Schon vor der Zusammenstellung der Liste wurde Deloitte im Bericht *Cyber Security Consulting 2013* von Kennedy Consulting Research and Advisory, einer führenden Analystenfirma, als ein weltweit führendes Unternehmen hinsichtlich der Beratung zur Cyber-Sicherheit bezeichnet.

Es ist nicht das erste Mal, dass die Risikodienstleistungen von Deloitte für ihre Expertise im Bereich Cyber-Sicherheit ausgezeichnet wurden. Im Laufe der letzten Monate haben bereits zahlreiche Analysten die Dienstleistungen des Unternehmens in den Bereichen Governance, Risiko und Compliance für die Beratung zu Risikomanagement, Sicherheit, Informationssicherheit usw. gewürdigt. Der Kennedy-Bericht betont die Effektivität des integrierten, vollumfänglichen Ansatzes, der von Deloitte gewählt wurde. Dieser ermöglichte die umfassendste Wissenssammlung auf dem Cyber-Sicherheitsmarkt.

Der Kennedy-Bericht führt weiter aus, dass „*Deloitte ein starkes Nutzenversprechen zur Cyber-Sicherheitsberatung einbringt, indem es seine Branchenkenntnisse, das Vorgehen „ein Ansatz, ein Modell“, spezielle Investitionen in die Cyber-Sicherheit und die Kommunikationsfähigkeiten auf Führungsebene miteinander verbindet.* “

About Deloitte

“Deloitte” is the brand under which tens of thousands of dedicated professionals in independent firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management, and tax services to selected clients. These firms are members of Deloitte Touche Tohmatsu Limited (DTTL), a UK private company limited by guarantee. Each member firm provides services in a particular geographic area and is subject to the laws and professional regulations of the particular country or countries in which it operates. DTTL does not itself provide services to clients. DTTL and each DTTL member firm are separate and distinct legal entities, which cannot obligate each other. DTTL and each DTTL member firm are liable only for their own acts or omissions and not those of each other. Each DTTL member firm is structured differently in accordance with national laws, regulations, customary practice, and other factors, and may secure the provision of professional services in its territory through subsidiaries, affiliates, and/or other entities.

About Deloitte in Luxembourg

In Luxembourg, Deloitte consists of 70 partners and over 1,600 employees and is amongst the leading professional service providers on the market. For over 60 years, Deloitte has delivered high added-value services to national and international clients. Our multidisciplinary teams consist of specialists from different sectors and guarantee harmonised quality services to our clients in their field. Deloitte General Services is a member of Deloitte Touche Tohmatsu Limited, one of the world’s leading professional services firms.