Deloitte General Services
Société à responsabilité limitée
560, rue de Neudorf
L-2220 Luxembourg
B.P. 1173
L-1011 Luxembourg

Tel: +352 451 451
Fax: +352 451 452 985
www.deloitte.lu

Press release

Fabienne Aßmann
Marketing & Communications
Tel: +352 451 452 422
Email: lupress@deloitte.lu

Businesses will experience cyber-attacks: Deloitte report outlines top threats for seven industries and provides tips to understand greatest risk

Advanced persistent threats have become a reality for all organisations that depend on digital technology

Today's senior executives must deploy a cyber-defense that is secure, vigilant, and resilient, according to a report recently released by Deloitte Touche Tohmatsu Limited (Deloitte Global). The report '*Global Cyber Executive Briefing'* finds that virtually all organisations will be attacked; that is why senior executives need to better understand their biggest threats and which assets – typically those at the heart of their business's mission – are at the greatest risk.

The report examines threats and vulnerabilities across seven key sectors: high technology, online media, telecommunications, e-commerce, insurance, manufacturing and retail. It outlines potential for attacks, reasons and possible scenarios as well as possible impacts on business.

"*Cyber-attacks should be a crucial concern for any company as they are not – as widely assumed – restricted to particular industries. All businesses with valuable data might be a future target for these threats having evolved with the Information Age,*" states Roland Bastin, partner at Deloitte Luxembourg. "*Therefore, it is important to be aware of potential risks, by not only knowing the value of your data but also by detecting potential adversaries and their operating methods, in order to ensure the most appropriate protection possible*."

According to the report, being **secure** starts with tackling weaknesses in applications and reinforcing the digital infrastructure. Organisations that are **vigilant** should subsequently be alert and identify any attacks as early as possible. Being **resilient** involves early-stage identification of the direction of a threat, the reason for such threat and how it will manifest itself. Rapidly detecting an attack can spur an organisation into action to isolate and remove the threat.

"*Knowing the key threats for your economic sector is a first important measure in order to be one step ahead of your potential attacker. That is why the Deloitte report focused on possible threats assessed for each of the seven main industries concerned,*" explains Stéphane Hurtaud, partner at Deloitte Luxembourg.

Highlights of the report, including threats by sector, involve:

- **High tech –** a consistent target for attacks with the biggest threats regarding the loss of intellectual property (IP) and hactivism. Threats are also used as a stepping stone to attack and infect others.
- **Online media** has the greatest exposure to cyber-threats with causing reputational damage topping the list. Threats are also used as a stepping stone to attack and infect others.
- The **telecommunications sector** is facing increased, sophisticated attacks, including those by Government agencies using Advanced Persistent Threats (APT) to establish covert surveillance for long periods of time. Another critical threat unique to the telecommunications sector is the attack of leased infrastructure equipment, such as home routers from Internet Service Providers (ISPs).
- **E-commerce**: Databases and online payment systems are vulnerable areas often attacked (e.g. leading to loss of customer data, including names, addresses, phone numbers). Denial-of-service attacks also top the list, particularly by hacktivists that want to disrupt an organization in a highly visible way.
- **Insurance:** The sector typically has a lot of sensitive data to protect. Cyber-attacks are growing exponentially as insurance companies migrate toward digital channels with sophisticated attacks combining advanced malware with other techniques such as social engineering. While current attacks appear only to be short-termed, the report predicts the number of long-term attacks to grow silently.
- **Manufacturing:** There is an increasing amount of attacks by hackers and cyber-criminals as well as through corporate espionage. Types of cyber-attacks in manufacturing vary widely from phishing to advanced malware, targeting not only IT but also connected industrial control systems.
- **Retail:** Credit card data is the new currency for hackers and criminals. Insider threats in retail are increasing, giving rise to a new breed of criminals that focus on stealing information – especially the valuable cardholder data that flows between consumers and retailers.

A complete version of the briefing is available on the Deloitte Luxembourg website: **http://www.deloitte.com/lu/global-cyber-executive-briefing**.

Les entreprises subiront des cyber-attaques: un rapport de Deloitte expose les principales menaces et fournit des conseils pour mieux comprendre les risques-clés

Des menaces persistantes avancées : une réalité pour toutes les entreprises dépendantes de la technologie numérique

La quasi-totalité des sociétés subiront des attaques cybernétiques, comme le révèle le rapport « Global Cyber Executive Briefing » récemment publié par Deloitte Touche Tohmatsu Limited (Deloitte Global). C'est pourquoi il est nécessaire que les dirigeants d'entreprise prennent conscience des principales menaces, identifient parmi leurs actifs stratégiques ceux qui sont le plus exposés et mettent en œuvre des procédures de cyberdéfense sécurisées, réactives et résistantes.

Le rapport met en exergue les menaces et vulnérabilités à travers sept secteurs-clés : high-tech, médias en ligne, télécommunications, e-commerce, assurance, industrie manufacturière et commerce de détail. Il étudie la probabilité des attaques, les raisons et les scénarios possibles ainsi que leur impact sur les sociétés.

« Les cyberattaques devraient constituer une préoccupation essentielle pour toute entreprise étant donné qu'elles ne se limitent pas à certains secteurs, comme souvent présumé. A l'ère de l'information, toute entreprise possédant des données sensibles risque d'être un jour ou l'autre exposée à ces menaces », explique Roland Bastin, partner chez Deloitte Luxembourg. « *Il importe dès lors d'être conscient des risques, non seulement en connaissant la valeur de ses données mais également en identifiant ses adversaires potentiels ainsi que leur mode opérationnel, afin de garantir une protection optimale.* »

Selon le rapport, **sécuriser** son environnement commence par la correction des failles des applications ainsi que le renforcement de l'infrastructure numérique. Des entreprises **vigilantes** devraient ensuite être alertes et identifier le plus tôt possible d'éventuelles attaques. Afin d'être **résistant** les dirigeants d'entreprise doivent identifier la menace, la raison ainsi que la manifestation éventuelle de cette dernière. Une société sera en mesure d'isoler et de contrer une menace si celle-ci a été détectée suffisamment tôt.

Stéphane Hurtaud, partner chez Deloitte Luxembourg : « *Il convient de connaître les principales menaces pesant sur votre secteur d'activité afin d'avoir une longueur d'avance sur les cybercriminels. C'est dans cette optique que le rapport de Deloitte s'est concentré sur les sept grands secteurs particulièrement ciblés par de telles attaques* ».

Conclusions du rapport pour chaque secteur d'activité :

- Le **high-tech** fait constamment les frais de cyberattaques, la perte de la propriété intellectuelle et l'hacktivisme constituant les principales menaces. Les cybercriminels utilisent souvent le secteur comme relais pour attaquer et infecter d'autres entités.
- Les **médias en ligne** sont les plus exposés aux cybermenaces, et principalement aux attaques portant atteinte à la réputation. Souvent, les cybercriminels utilisent également le secteur comme relais pour attaquer et infecter d'autres entités.
- Les **télécommunications** sont confrontées à un nombre croissant d'attaques de plus en plus sophistiquées, notamment de la part d'agences gouvernementales qui recourent aux menaces persistantes avancées (APT) pour exercer une surveillance discrète sur des périodes prolongées. Le secteur fait également face à une menace critique qui lui est

propre, à savoir les attaques visant les équipements d'infrastructure en location, tels que les routeurs domestiques des fournisseurs de services Internet.

- Dans le secteur de l'**e-commerce**, les bases de données (perte de données clients telles que le nom, l'adresse postale, le numéro de téléphone, etc.) et les systèmes de paiement en ligne font souvent les frais de cyberattaques du fait de leur vulnérabilité. Les attaques visant à interrompre les services figurent également en tête de liste et proviennent bien souvent d'hacktivistes cherchant à perturber publiquement les activités d'une entreprise.
- Le secteur de l'**assurance** doit protéger bon nombre de données sensibles. Les cyberattaques se multiplient à un rythme exponentiel alors que les compagnies d'assurance se tournent vers des canaux numériques. Les criminels font preuve d'inventivité en combinant des logiciels malveillants avancés à d'autres techniques telles que l'ingénierie sociale. Si les attaques actuelles semblent de court terme, le rapport prévoit que le nombre d'attaques à long terme devrait augmenter silencieusement.
- L'**industrie manufacturière** est de plus en plus la cible de hackers et de cybercriminels et l'espionnage industriel y est monnaie courante. Les cyberattaques visant le secteur sont très variées (hameçonnage, logiciels malveillants avancés, etc.) et ne concernent pas uniquement l'informatique mais également les systèmes de contrôle industriel connectés.
- Dans le secteur du **commerce de détail**, les données relatives aux cartes de crédit constituent la nouvelle monnaie d'échange entre hackers et criminels. Les risques de fuite en interne se multiplient, ce qui donne naissance à un nouveau type de criminels adeptes du vol d'informations, notamment en ce qui concerne les données bancaires qui circulent entre consommateurs et vendeurs.

La version complète du rapport est disponible sur le site de Deloitte Luxembourg : **http://www.deloitte.com/lu/global-cyber-executive-briefing**.

Bevorstehende Cyber-Attacken: Deloitte-Bericht stellt wesentliche Bedrohungen für sieben Branchen dar und gibt Tipps zum besseren Verständnis der größten Risiken

*Fortgeschrittene, andauernde Bedrohungen (***Advanced Persistent Threats***) sind für alle Organisationen, die von digitaler Technologie abhängig sind, zur Realität geworden*

Der Einsatz einer sicheren, wachsamen und widerstandsfähigen Cyber-Abwehr ist für Unternehmen heutzutage unumgänglich – das geht aus einem kürzlich veröffentlichten Bericht von Deloitte Touche Tohmatsu Limited (Deloitte Global) hervor. Laut dem *„Global Cyber Executive Briefing"* sind Organisationen aller Wirtschaftsbereiche von der Bedrohung betroffen. Aus diesem Grund müssen leitende Führungskräfte ein besseres Verständnis dafür entwickeln, wo die größten Bedrohungen für ihr Unternehmen liegen und welche Aktiva – vor allem solche, die ihr Kerngeschäft betreffen – den größten Risiken ausgesetzt sind.

Der Bericht untersucht Bedrohungen und Anfälligkeiten in sieben wichtigen Branchen: High-Tech, Online-Medien, Telekommunikation, E-Commerce, Versicherungswesen, verarbeitendes Gewerbe und Einzelhandel. Beleuchtet werden Angriffspotenzial, Hintergründe und damit verbundene mögliche Szenarien sowie etwaige Geschäftsauswirkungen.

„Cyber-Angriffe müssen von jedem Unternehmen sehr ernst genommen werden, da sie nicht – wie allgemein angenommen – auf bestimmte Branchen beschränkt sind. Alle Unternehmen, die wertvolle Daten besitzen, können ein künftiges Ziel solcher Bedrohungen sein, die das Informationszeitalter hervorgebracht hat", erläutert Roland Bastin, Partner bei Deloitte Luxemburg. *„Deshalb ist es für Unternehmen wichtig, sich der potenziellen Risiken bewusst zu sein, indem sie nicht nur den Wert ihrer Daten kennen, sondern auch, indem sie potenzielle Feinde und ihre Vorgehensweisen identifizieren, um den bestmöglichen Schutz sicherzustellen."*

Sicher bedeutet laut dem Bericht, die Schwachstellen in Anwendungen herauszufinden und die digitale Infrastruktur zu verbessern. **Wachsam** sind Organisationen dann, wenn sie alarmbereit sind und Angriffe so früh wie möglich erkennen. **Schlagkräftig** impliziert das frühzeitige Erkennen der Richtung einer Bedrohung, deren Hintergrund und wie sie sich manifestieren wird. Das schnelle Aufdecken eines Angriffs ermöglicht der Organisation ein umgehendes Handeln, um die Bedrohung zu isolieren und zu beseitigen.

„Die Hauptbedrohungen Ihres Wirtschaftssektors zu kennen, ist eine erste, wichtige Maßnahme, um Ihrem potenziellen Angreifer einen Schritt voraus zu sein. Aus diesem Grund lag der Schwerpunkt des Berichts auf der Erörterung möglicher Bedrohungen, die jeweils für die sieben anfälligsten Branchen ermittelt wurden", erklärt Stéphane Hurtaud, Partner bei Deloitte Luxemburg.

Wesentliche Schlussfolgerungen des Berichts, einschließlich der Bedrohungen nach Sektoren:

- **High-Tech –** ständiges Ziel für Attacken mit den größten Gefahren im Hinblick auf Verlust von geistigem Eigentum und Hackerangriffen. Bedrohungen werden auch als Sprungbrett verwendet, um andere anzugreifen und zu infizieren.
- **Online-Medien** sind den größten Risiken durch Cyber-Bedrohungen ausgesetzt. Dabei steht Rufschädigung an oberster Stelle der Liste. Bedrohungen werden ebenfalls als Sprungbrett verwendet, um andere anzugreifen und zu infizieren.

- **Telekommunikation**: Der Sektor ist mit zunehmenden, ausgeklügelten Attacken konfrontiert. Dazu gehören auch solche von Regierungsstellen, die *Advanced Persistent Threats* (APT) verwenden, um eine geheime Überwachung über längere Zeiträume hinweg zu etablieren. Eine andere kritische Bedrohung, die ausschließlich den Telekommunikationssektor betrifft, ist der Angriff auf geleaste Infrastrukturausrüstung, wie Home-Router von Internet Service Providern (ISPs).
- **E-Commerce**: Datenbanken und Online-Zahlungssysteme sind anfällige Bereiche, die häufig angegriffen werden (und führen z.B. Verlust von Kundendaten, einschließlich Namen, Anschriften, Telefonnummern). Angriffe, die Dienstleistungsverhinderungen bewirken (*Denial of Service*-Angriffe) und insbesondere durch Hacker verursacht werden, die eine Organisation auf sehr transparente Weise stören möchten, rangieren ebenfalls oben auf der Liste.
- **Versicherungswesen:** Diese Branche hat besonders umfangreiche, sensible Daten zu schützen. Cyber-Attacken nehmen exponentiell zu, da Versicherungsunternehmen auf digitale Kanäle umstellen. Ausgeklügelte Attacken verbinden dabei hochentwickelte schädliche Software (*Advanced Malware*) mit anderen Techniken wie beispielsweise *Social Engineering* (Manipulation von Benutzern zur Erlangung vertraulicher Informationen). Während derzeitige Attacken eher kurzfristiger Natur sind, wird die Zahl der langfristigen Attacken gemäß der Vorhersage des Berichts schleichend zunehmen.
- **Verarbeitendes Gewerbe:** Die Zahl der Cyber-Angriffe durch Hacker und Cyber-Kriminelle sowie durch Unternehmensspionage nimmt zu. Die Arten der Cyber-Angriffe im verarbeitenden Gewerbe sind vielfältig, von *Phishing* bis zu *Advanced Malware*, und zielen nicht nur auf IT, sondern auch auf damit verbundene industrielle Kontrollsysteme ab.
- **Einzelhandel:** Kreditkartendaten sind die neue Währung für Hacker und Kriminelle. Die Insider-Bedrohungen im Einzelhandel nehmen zu und fördern einen neuen Typ von Kriminellen, die sich auf Datendiebstahl konzentrieren – insbesondere von wertvollen Kartenhalterdaten, die zwischen Verbrauchern und Einzelhändlern ausgetauscht werden.

Eine vollständige Version des Briefings finden Sie auf der Deloitte Luxembourg Webseite: **http://www.deloitte.com/lu/global-cyber-executive-briefing**.