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

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

Deloitte Luxembourg and EBRC look into the cyber security journey - think early, act effectively and react promptly

Most security breaches are still perpetrated by external attackers and the financial services industry is particularly exposed to security incidents with confirmed data loss. This was one of the findings of the Verizon 2014 Data Breach Investigations Report (DBIR), presented at the Cyber Security conference, organised by Deloitte Luxembourg and EBRC.

Attracting close to 50 security and IT professionals, risk managers, internal auditors, among others, the conference aimed to provide the latest updates on the cyber threat landscape and focus on the typical approaches, standards, regulations and capabilities to protect organisations from cyber threats.

The digital revolution is driving business innovation and growth, yet also exposing all organisations to new and emerging threats. Indeed, organisations must face a myriad of threat agents, whose determination and attacking resources may greatly vary from one to another.

Stéphane Hurtaud, Partner at Deloitte Luxembourg explained *"The threat landscape has changed, and the need for more mature cyber security is higher than before. In today's world, addressing cyber security risks with point solutions is clearly unrealistic. Given the complexity of the cyber risk landscape, one must adopt a much more cohesive and structured approach for managing your cyber risks effectively"*.

Moving from information security to risk intelligent security
The 2014 DBIR provides information on attackers, their motivation, demography and methods that can help companies to protect their most valuable assets. The latest edition of this report confirms that, whilst most security breaches come from the outside, the main motive of the threat remains financial gain, even if industrial espionage has been rising over the last few years.

Sebastien Besson, Cyber Security specialist at Deloitte, also emphasised that *"It takes less and less time for an attacker to compromise his/her target. Some 60% of security incidents occur within a couple of hours, whereas 62% of incidents are discovered months later."*

During the conference, speakers discussed this complex and ever-evolving threat landscape, concluding that organisations need to adopt a cohesive approach to protection from cyber threats, underpinned by 5 key principles:

- Understand risk exposition and defining the risk appetite
- Ensure close alignment with business goals
- Prepare for the worst

- Share intelligence
- Instil a broad awareness of cyber security

The prevalence and sophistication of recent cyber attacks on public and private organisations highlight a number of capabilities that are essential to cyber security (from prevention to detection).

Leveraging the National Institute of Standards and Technology (NIST) cybersecurity framework

The speakers also addressed the question of how a company should react towards constant reports of cyber security breaches.
Régis Jeandin (EBRC, Head of Security Services) confirmed that: "*Too often, a pragmatic and structured approach towards cyber security could save time and be cost effective, however, taking the time to step aside and initiate a true reflexion is lacking in many organisations*."

The conference was an opportunity for the audience to review one of the most recent frameworks in cyber security and its three corner stones:

1. Definition of the core functions (identification, protection, detection, response, recovery)
2. Definition of the current situation (e.g. profile) and target. This profiling allows companies to identify the gaps and initiate the relevant action plans
3. Definition of the 'tiers' (tier 4 being most secure and tier 1 being least secure), through which the characteristics of the organisation's approach to risk is evaluated

Cyber incident response: challenges and solutions

To become more efficient and to better protect valuable IT assets against the continuously evolving cyber threats, information security should adopt a new form, moving from traditional perimeter protection to rapid and advanced detection and response capabilities to a cyber security incident.

Matthijs van der Wel, Director of the Incident Response department at DataExpert, explained that often, it takes 2 weeks for an organisation to perform computer forensics analysis of one single compromised system in its environment. He further added that companies often lack strong incident response capabilities, enabling them to timely react to an adverse security event. Most of the efforts spent on information security today still focus mainly on preventive measures. Through examples, he showed that latest cyber attacks demonstrate that prevention is not sufficient anymore to ensure the adequate protection of systems and networks.

During his presentation, Matthijs provided an overview of new existing incident response solutions, using specific software agent deployed on corporate computer systems. Such solutions enable organisations to react faster to a security incident, by:

1. Performing computer forensics analysis from a remote location
2. Analysing the state of multiple systems across the company, using a set of various data sources (e.g. network, operating system, application information) to detect any anomaly which could be a potential indicator of a successful security breach
3. Restoring previous states of a given system back in time, to better pinpoint the timeframe and the source of a security incident

Deloitte Luxembourg et EBRC embarquent sur le vaisseau de la cybersécurité : anticipation, intervention efficace et réaction rapide

La plupart des attaques portées aux réseaux informatiques demeurent le fait d'assaillants externes et les services financiers, en tant que secteur, se trouvent en première ligne des incidents en termes de sécurité, avec à la clé des pertes de données avérées. Telle fut l'une des conclusions du Verizon 2014 Data Breach Investigations Report (DBIR), présenté lors de la conférence Cyber Security organisée par Deloitte Luxembourg et EBRC.

Rassemblant près d'une cinquantaine de professionnels de la sécurité et de l'IT, de risk managers, de réviseurs internes, et autres, la conférence avait pour objectif de faire le point sur les dernières évolutions observées dans le paysage des menaces cybernétiques et de se concentrer sur les approches, normes, réglementations et capacités qui entourent généralement la protection des organisations face aux menaces des réseaux informatiques.

Si elle se veut le moteur de l'innovation et de la croissance des affaires, la révolution numérique expose aussi chaque organisation à des dangers, qu'ils soient nouveaux ou émergents. Les entreprises doivent en effet faire face à une multitude de vecteurs de menace, dont les motivations et les ressources peuvent être très différentes.

Stéphane Hurtaud, Partner chez Deloitte Luxembourg : *« Le paysage a évolué et une maturité accrue de la sécurité des réseaux se fait de plus en plus indispensable. Dans le monde actuel, il n'est plus réaliste d'aborder la cybersécurité par le biais de solutions ponctuelles. Compte tenu de la complexité des menaces, il convient d'adopter une approche nettement plus cohérente et structurée pour gérer efficacement les risques cybernétiques. »*

De la sécurité des informations à une protection intelligente contre les risques
Le rapport DBIR 2014 se penche sur le profil des assaillants, leur motivation, la démographie ainsi que sur les méthodes susceptibles d'aider les entreprises à protéger leurs actifs les plus précieux. La dernière édition du rapport confirme que, si la plupart des violations de sécurité proviennent de l'extérieur, la motivation première des pirates informatiques demeure l'appât du gain, même si l'espionnage industriel s'intensifie ces dernières années.

Sébastien Besson, spécialiste de la cybersécurité chez Deloitte : *« Il faut de moins en moins de temps à un assaillant pour atteindre sa cible. Environ 60% des incidents se produisent en quelques heures seulement, alors que 62% d'entre eux ne sont détectés qu'après plusieurs mois. »*

Au cours de la conférence, les intervenants sont revenus sur la complexité et l'évolution perpétuelle des menaces, concluant que les organisations doivent adopter une approche cohérente de la protection des réseaux, qui s'appuie sur 5 principes fondamentaux :

- Comprendre l'exposition aux risques et définir l'appétit pour le risque
- Garantir un alignement fidèle vis-à-vis des objectifs de l'entreprise
- Se préparer au pire
- Partager les savoirs
- Sensibiliser le plus largement possible à la sécurité des réseaux

La fréquence et la sophistication des attaques récentes perpétrées contre des organisations publiques et privées mettent en évidence un certain nombre de capacités essentielles dans le cadre de la sécurité informatique (de la prévention à l'identification).

Exploiter le cadre de référence en matière de cybersécurité édicté par l'Institut national des normes et de la technologie (NIST)
Les participants se sont également intéressés à la réaction que devraient avoir les sociétés face aux nombreuses violations de sécurité rapportées.
Régis Jeandin (EBRC, Head of Security Services) : *« Il arrive très souvent qu'une approche pragmatique et structurée de la sécurité des réseaux suffise à faire gagner du temps et de l'argent aux organisations. Cependant, pour bon nombre d'entre elles, c'est le temps nécessaire pour prendre du recul et entamer une véritable réflexion qui fait défaut. »*

La conférence a donné l'occasion aux participants de passer en revue l'un des cadres les plus récents de la cybersécurité et ses trois pierres angulaires :

1. Définition des fonctions clés (identification, protection, détection, réaction, réparation) ;
2. Définition de la situation actuelle (profil) et visée. Ce profilage permet aux sociétés d'identifier les carences et d'initier les plans d'action adéquats ;
3. Définition de paliers (« tiers »), du palier 4 (le plus sécurisé) au palier 1 (le moins sécurisé), permettant d'évaluer les caractéristiques de l'approche de l'organisation à l'égard des risques.

Réaction à un incident cybernétique : défis et solutions

Pour gagner en efficacité et offrir une meilleure protection des précieux actifs IT face à des menaces cybernétiques en perpétuelle évolution, il est temps d'adopter une nouvelle approche de la sécurité des informations et d'évoluer d'une protection périphérique traditionnelle à une détection rapide et poussée et de meilleures capacités de réaction à un incident de sécurité des réseaux.

Matthijs van der Wel, Directeur du département Incident Response chez DataExpert, explique qu'il faut parfois deux semaines pour qu'une organisation effectue une analyse informatique complète d'un système ayant fait l'objet d'une attaque dans son environnement. Il ajoute que les entreprises ne disposent bien souvent tout simplement pas des capacités de réaction suffisantes qui leur permettraient de réagir à temps à un événement affectant leur sécurité. La plupart des efforts consacrés à la sécurité des informations aujourd'hui continuent de se concentrer principalement sur les mesures de prévention. A travers différents exemples, il a démontré que les dernières attaques cybernétiques ont mis en évidence le fait que la prévention n'était plus suffisante pour garantir une protection adéquate des systèmes et des réseaux.

Durant son exposé, M. van der Wel s'est attelé à présenter les nouvelles solutions de réponses à un incident, en faisant appel à un agent logiciel spécifique déployé sur les systèmes informatiques des entreprises. Ce type de solutions permet aux organisations de réagir plus rapidement à un incident de sécurité, notamment par le biais de :

1. L'exécution d'analyses informatiques depuis un emplacement distant
2. L'analyse de l'état de plusieurs systèmes à travers la société en faisant appel à toute une série de sources de données (réseaux, système d'exploitation, informations sur les applications) afin de détecter toute anomalie qui pourrait indiquer qu'une attaque a été perpétrée avec succès
3. La restauration d'un système donné à un point antérieur dans le temps, afin de localiser avec plus de précision le moment et la source d'un incident en termes de sécurité.

Deloitte Luxemburg und EBRC erörtern Cybersicherheit
– früh nachdenken, effizient handeln und schnell reagieren

Der Finanzdienstleistungssektor ist wie kaum eine andere Branche von Sicherheitsverletzungen betroffen. Diese werden in erster Linie von externen Akteuren begangen. Dabei kommt es häufig auch zum Verlust von Daten. Dies war eines der Ergebnisse des Verizon 2014 Data Breach Investigations Report (DBIR), der auf der von Deloitte Luxemburg und EBRC organisierten Konferenz für Cybersicherheit vorgestellt wurde.

Die Konferenz, auf der knapp 50 Sicherheits- und IT-Experten, Risikomanager, interne Revisoren und andere Fachleute zusammenkamen, hatte zum Ziel, die neuesten Entwicklungen bei Cyberrisiken sowie die wichtigsten Ansätze, Standards, Vorschriften und Kapazitäten zu erörtern, mit denen sich Unternehmen und Organisationen vor Cyberbedrohungen schützen können.

Die digitale Revolution treibt Innovation und Wachstum voran, setzt jedoch alle Organisationen auch neuen Bedrohungen durch Hacker aus. Diese können sich in ihrer Entschlossenheit und ihren Ressourcen stark voneinander unterscheiden.

Stéphane Hurtaud, Partner bei Deloitte Luxemburg, erklärte dazu: *„Die Gefahrenlandschaft hat sich verändert, und der Bedarf an ausgereifteren Sicherheitssystemen ist größer denn je. In der heutigen Welt ist es unrealistisch, Cybersicherheit durch Punktlösungen zu erreichen. Angesichts der Vielfalt an Cybergefahren ist es erforderlich, einen einheitlicheren und strukturierteren Ansatz für den effizienten Umgang mit diesen Risiken zu wählen."*

Von der Informationssicherheit zur Sicherheit durch Risikobewusstsein
Der 2014 DBIR bietet Informationen über Angreifer, ihre Motive und ihren soziodemografischen Hintergrund sowie über Methoden, mit denen Unternehmen ihr wertvollstes Kapital besser schützen. Die neueste Ausgabe des Berichts bestätigt, dass die Sicherheitsverletzungen vornehmlich von außerhalb kommen und dass es trotz einer Zunahme der Industriespionage in den vergangenen Jahren den meisten Angreifern hauptsächlich darum geht, finanzielle Vorteile zu erlangen.

Wie Sebastien Besson, Spezialist für Cybersicherheit bei Deloitte, betonte: *„Angreifer benötigen immer weniger Zeit, um ihr Zielobjekt zu schädigen. Obwohl sich etwa 60% der Sicherheitsvorfälle innerhalb weniger Stunden ereignen, werden 62% der Vorfälle erst Monate später entdeckt."*

Während der Konferenz erörterten die Redner diese komplexe und sich ständig wandelnde Gefahrenlandschaft und kamen zu dem Schluss, dass Unternehmen einen kohärenteren Ansatz wählen müssen, um sich besser vor Cybergefahren zu schützen. Dabei wurden fünf Schlüsselprinzipien besonders hervorgehoben:

- Kenntnis der vorhandenen Risiken und Festlegung der Risikoneigung
- Ausrichtung der Prozesse an den Geschäftszielen
- Vorbereitung auf das „Worst-Case-Szenario"
- Informationsaustausch
- Entwicklung eines Bewusstseins für die Cybersicherheit

Die Häufigkeit und die ausgeklügelte Natur der jüngsten Cyberangriffe auf öffentliche und private Organisationen zeigen, dass eine Reihe von Fähigkeiten erforderlich sind, um die Cybersicherheit zu gewährleisten (von der Prävention bis hin zur Erkennung).

Nutzung des Netwerks für Cybersicherheit des National Institute of Standards and Technology (NIST)
Die Redner beschäftigten sich außerdem mit der Frage, wie ein Unternehmen auf Berichte über die ständige Verletzung der Cybersicherheit reagieren sollte.
Régis Jeandin (EBRC, Head of Security Services) bestätigte: *„In vielen Fällen würde ein pragmatischer und strukturierter Ansatz bei der Cybersicherheit Zeiteinsparungen und*

Effizienzgewinne ermöglichen. Allerdings fehlt es in vielen Unternehmen an der nötigen Zeit, um sich in Ruhe mit dem Thema auseinanderzusetzen.“
Die Konferenz bot dem Publikum die Gelegenheit, eines der neuesten Rahmenwerke bei der Cybersicherheit und seine drei Eckpfeiler zu erörtern:

1. Definition der Kernfunktionen (Identifikation, Schutz, Erkennung, Reaktion, Erholung)
2. Definition der aktuellen Situation (d.h. Profil) und Ziel. Dieses Profiling erlaubt es Unternehmen, die bestehenden Lücken zu erkennen und entsprechende Aktionspläne einzuleiten.
3. Definition der Tiers (wobei Tier 4 am sichersten und Tier 1 am unsichersten ist), anhand derer der Ansatz des Unternehmens beim Umgang mit Risiken bewertet wird

Reaktion auf Cybervorfälle: Herausforderungen und Lösungen
Um effizienter zu werden und wertvolle IT-Ressourcen vor den sich ständig wandelnden Cyberbedrohungen zu schützen, sollte die Informationssicherheit eine neue Form annehmen: Der traditionelle Perimeterschutz muss durch eine moderne Erkennung und Reaktion auf Cybersicherheitsvorfälle ersetzt werden.

Laut Matthijs van der Wel, Leiter der Abteilung Incident Response bei DataExpert, benötigen Unternehmen häufig zwei Wochen, um eine Computer-Forensik durchzuführen, selbst wenn nur ein einziges System ihrer Umgebung betroffen ist. Er fügte hinzu, dass es den Unternehmen häufig an den erforderlichen Kapazitäten fehlt, um rechtzeitig auf Sicherheitsvorfälle zu reagieren. Die meisten Anstrengungen im Zusammenhang mit der Informationssicherheit konzentrieren sich heute vornehmlich auf präventive Maßnahmen. Anhand mehrerer aktueller Beispiele von Cyberangriffen zeigte der Experte, dass jedoch vorbeugende Maßnahmen alleine nicht mehr ausreichen, um Systeme und Netze zu schützen.

Während seiner Präsentation bot er einen Überblick über neue Lösungen, wie Unternehmen mittels spezifischer Software-Agenten auf ihren Computersystemen schneller und besser auf Cybervorfälle reagieren können. Diese Programme versetzen die Unternehmen in die Lage:

1. forensische Computeranalysen von einem entfernten Standort aus durchzuführen
2. den Zustand verschiedener Systeme innerhalb des Unternehmens zu analysieren, unter Nutzung unterschiedlicher Datenquellen (z.B. Netzwerke, Betriebssysteme, Anwendungsdaten); dadurch lassen sich Anomalien erkennen, die als potenzielle Indikatoren einer erfolgreichen Sicherheitsverletzung dienen
3. den vorherigen Zustand des Systems wiederherzustellen, um Zeitpunkt und Urheber des Sicherheitsverstoßes besser ermitteln zu können

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 80 partners and over 1,500 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.