GASTKOLUMNE

ICT – SICHERHEITSANFORDERUNG VERSUS EIGENE SENSIBILITÄT

FRIDEL RICKENBACHER, MIT-GROUP
FRIDEL.RICKENBACHER@MIT-GROUP.CH

Alle polemisieren über grosse Sicherheitsrisiken im ICT-Bereich und speziell bei Cloud-Services – folgend einige Gedankenanstösse dazu.

Die ICT-Gesamtsicherheit, beziehungsweise letztlich die ICT-Strategie, ist ein umfassender Prozess auf der Führungsebene und nicht nur eine Ansammlung von Technologien, Produkten und Tools. Der *Sicherheitsfaktor Mensch* ist unter diesem Aspekt und aus statistisch belegbarer Erfahrung wichtiger und heikler als der *Faktor Maschine* oder die technische Infrastruktur. Folgend einige Fragestellungen zur Relation der Problematik und zu den erkennbaren Anknüpfpunkten:

- Welche firmen- und personensensitive Daten werden täglich via Social Media, Online-Plattformen und E-Mail von *Menschen* und eben nicht von *Maschinen* publiziert?
- Bestehen intern überhaupt Weisungen, Sicherheitsrichtlinien und Geheimhaltungsvereinbarungen im Umgang mit der EDV und insbesondere mit dem Internet? Sind diese verbindlicher Bestandteil des Arbeitsvertrages?
- Gibt es eine spezielle ICT-Security-Policy oder einen internen Sicherheitverantwortlichen für den ICT-Bereich? (Schliesslich gibt es ja auch Sicherheitsverantwortliche zum Beispiel bei Bauunternehmungen, Baustellen, Produktionen et cetera).
- Werden die Mitarbeiter speziell sensibilisiert oder geschult für die sehr dynamischen Informatik-Sicherheits-Belange?
- Besteht ein Datensicherungskonzept mit externer Aufbewahrung der Sicherungsmedien?
- Ist die Führungsebene eingebunden (auf Stufe GL und VR) in die Strategiedefinition, Planung von ICT-Um-

LA PAGE DE L'INVITÉ

TIC – LES EXIGENCES DE SÉCURITÉ VS. LA SENSIBILITÉ PERSONNELLE

FRIDEL RICKENBACHER, MIT-GROUP
FRIDEL.RICKENBACHER@MIT-GROUP.CH

Polémique générale sur les importants risques de sécurité dans le domaine des TIC et notamment dans les services en nuage – quelques réflexions.

La sécurité globale des TIC, et en fin de compte la stratégie en matière de TIC, constitue un processus approfondi traité au niveau des cadres dirigeants, et pas seulement une accumulation de technologies, de produits et d'outils. Sous cet angle, et comme la statistique le prouve, le *facteur humain* est plus important et plus délicat pour la sécurité que le *facteur machine* ou que les infrastructures techniques. Voici quelques questions concernant la relation entre cette question et les connecteurs observables:

- Quelles sont les données sensibles concernant des personnes physiques et morales qui sont publiées quotidiennement par des *individus* et justement pas par des *machines* sur les réseaux sociaux, dans les plates-formes en ligne et par le biais de courriels?
- Est-ce qu'il existe en interne des directives de sécurité et des conventions de confidentialité pour la gestion de l'informatique et en liaison avec Internet? Font-elles partie intégrante et contraignante du contrat de travail?
- Existe-t-il une politique de sécurité spécifique TIC ou un responsable interne de la sécurité pour le domaine TIC? (Il existe aussi des responsables de la sécurité par ex. dans les entreprises de construction, sur les chantiers, dans les productions, etc.)
- Les collaborateurs sont-ils sensibilisés ou formés aux questions très dynamiques de sécurité informatique?
- Est-ce qu'il existe un concept d'archivage des données avec conservation externe des supports de sauvegarde?
- Les cadres dirigeants sont-ils impliqués (au niveau

gebungen, deren Sicherheits-Vorgaben und Controlling-Mechanismen wie IKS- oder Risk-Management?
- Werden auftrags- oder firmensensible Daten geschützt ausgetauscht mit Externen?

Wie man unschwer in den Fragen erkennen kann, wurden eigentlich noch gar keine Fragen nach den externen «bösen» Hackern, den spionierenden Staaten oder der «unsicheren» Cloud gestellt.
Die Gesamtsicherheit ist in einem entsprechenden Gesamtrahmen zu sehen – sie beginnt aber sicherlich in der internen, selbstkritischen Betrachtung von eigenen Prozessen und Infrastrukturen. Erst danach – beziehungsweise wenn das bereinigt, geklärt, definiert und kontrolliert ist – sollte man den Fokus erweitern in Richtung der externen Abhängigkeiten, Hackern, Internet, Cloud et cetera.
Eine hundertprozentige Sicherheit bei Mensch und Maschine gibt es nicht und wird es nie geben. Und genau das ist die Aufgabe der Führungsebene oder Kontrollgremien (Audit, IKS, Controlling): Diese übrig bleibenden Restrisiken zu identifizieren, klassifizieren, bewerten, zu testen und mit gangbaren präventiven Massnahmen und Prozessen zu reduzieren und sporadisch im Risk-Management zu prüfen.
Die entsprechende Schulung und der Schutz von Anwendern oder Risk-Management-Verantwortlichen – speziell auch der Sensibilisierung zur aktiven Mitarbeit im Thema Sicherheit – ist dabei ein entscheidender Faktor, um nicht in organisatorisch verhinderbare, firmenkritische Sicherheitsrisiken zu geraten.
Aus diesen Aspekten heraus empfehle ich: Bevor ein externer, technischer Schutzwall aufgebaut wird, sollte man als vorherige und dringlichere Basis die internen Prozesse, die Sicherheit und das Risk-Management kritisch überprüfen und anpassen. ■

Direction et CA) dans la définition de la stratégie, la planification des environnements TIC, leurs règles de sécurité et leurs mécanismes de controlling tels que SCI ou gestion des risques?
- Est-ce que les données sensibles pour un mandat ou l'entreprise sont échangées avec des personnes de l'extérieur de manière protégée?

Comme ce qui précède le montre, nous n'avons même pas encore posé de question sur les «méchants» pirates externes, les Etats espions ou les «déficiences de sécurité» des services nuage. La sécurité globale doit être replacée dans un cadre général approprié, mais ce qui est sûr, c'est quelle commence par l'observation interne et autocritique des processus et infrastructures de l'entreprise. Ce n'est qu'ensuite, dès que ces points ont été tirés au clair, définis et contrôlés, que l'on doit élargir le champ et passer aux dépendances externes, aux hackers, à Internet, au Cloud, etc.
La sécurité absolue en face des actions humaines et de machine n'existe pas et n'existera jamais. Et c'est justement là qu'intervient la tâche des cadres dirigeants ou des organes de contrôle (audit, SCI, controlling): il s'agit d'identifier, d'évaluer, de tester ces risques résiduels, de les réduire par des mesures préventives praticables et de les contrôler sporadiquement dans le cadre de la gestion des risques.
La formation correspondante et la protection des utilisateurs ou des responsables de la gestion des risques, y compris la sensibilisation à la collaboration active en faveur de la sécurité, constituent un facteur décisif pour ne pas exposer l'entreprise à de graves risques de sécurité qu'une bonne organisation permettrait d'éviter.
Pour toutes ces raisons, voici ma recommandation: avant de construire un mur de protection externe par des moyens techniques, il est plus urgent de commencer par examiner d'un œil critique et par adapter les processus internes, la sécurité et la gestion des risques. ■

Fridel Rickenbacher ist Mitbegründer, Partner und Verwaltungsrat der *MIT-Group*, einem Totalunternehmen für Informations- und Kommunikationsmanagement. Er absolvierte seine Ausbildung in den Bereichen Bauleiter/Projektleiter/Immobilienverwaltung (FH Horw) und Wirtschaftsinformatik/Engineering (HSLU) und ist seit über dreizehn Jahren Mitglied in der Informatikkommission des SIA.

Fridel Rickenbacher est cofondateur, associé et membre du conseil d'administration de MIT-Group, une entreprise totale de gestion de l'information et de la communication. Il a une formation de chef de chantier/chef de projet/administrateur immobilier (FH Horw) et en informatique économique/Ingénierie (HSLU) et il est depuis plus de 13 ans membre de la commission informatique de la SIA.

In den Gastkolumnen publizieren wir jeweils die Meinung wechselnder Autoren zu aktuellen Themen. Es handelt sich dabei weder um die Meinung der Redaktion, noch um die Haltung des SIA.

Dans les colonnes de l'invité, divers auteurs s'expriment sur des thèmes actuels. Leurs réflexions n'engagent pas la Rédaction et ne reflètent pas les positions de la SIA en la matière.