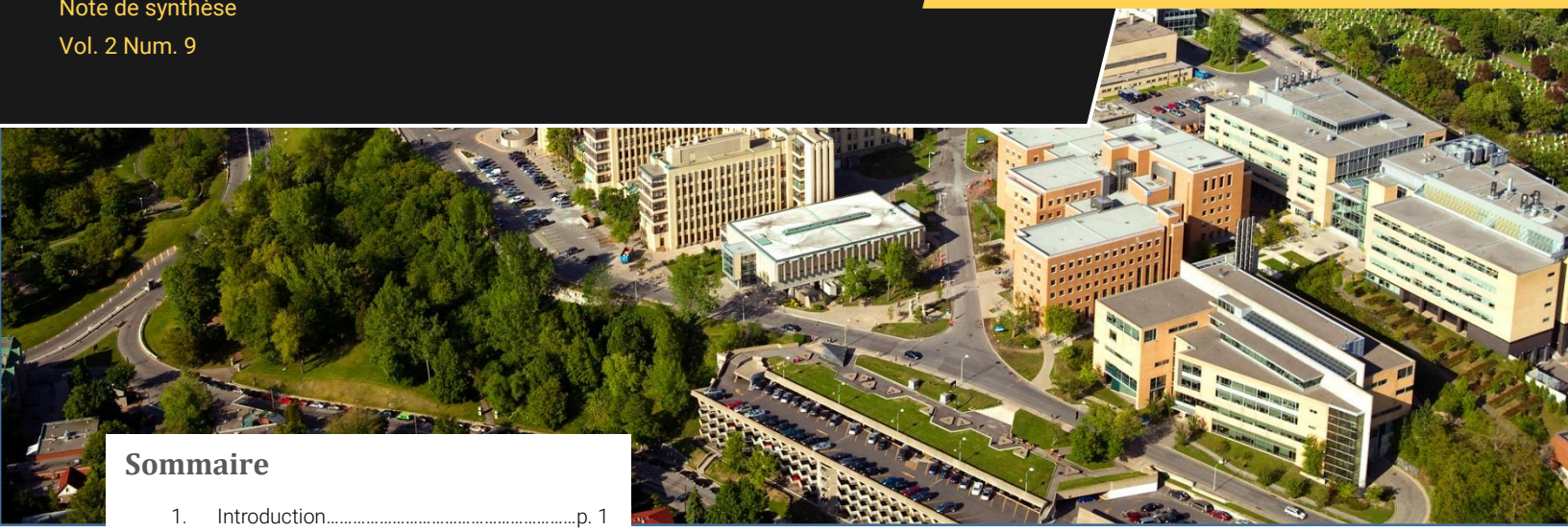
Les systèmes de détection d'intrusion

Traian Toma, candidat à la maîtrise

Note de synthèse
Vol. 2 Num. 9

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Introduction

La problématique de la menace interne rappelle aux organisations que, parfois, la source de cybermenaces est déjà nichée en leur sein[1]. Ainsi, les études portant sur la détection et la prédiction de la menace interne se sont accrues après la médiatisation du cas Snowden en 2013[2]. Les procédés de surveillance des systèmes et réseaux informatiques— déployés par près de la moitié des entreprises canadiennes[3] — ont d'ailleurs été adaptés afin d'essayer d'identifier les employés malintentionnés[4].

Les systèmes de détection d'intrusion (SDI) sont des outils qui parcourent les systèmes ou réseaux informatiques à la recherche de caractéristiques indicatrices d'une violation des politiques de sécurité et les signalent aux analystes de cybersécurité[5].

L'implantation par les organisations de SDI se caractérise par la volonté de dissuader les employés malveillants, mais leur mise en place peut en revanche exacerber la menace interne si elle ne tient pas compte des réactions négatives possibles.

Un premier portrait des SDI

Il existe deux types de SDI, chacun utilisant des données différentes :

- Les **SDI réseaux** analysent les informations qui sont généralement encapsulées dans des paquets, parcourant un réseau à n'importe quel moment donné[6]. Ces paquets contiennent entre autres les adresses IP expéditrices et récipiendaires liées aux informations en question.

- Les **SDI hôtes** recueillent les données des ordinateurs individuels (les appels système, les dynamiques de frappe de clavier ou de la souris, la journalisation, la base de registre, etc.).

La majorité des études scientifiques recommande les SDI hôtes pour lutter contre la menace interne, car les employés malintentionnés sont déjà présents sur le réseau de l'entreprise et peuvent, par exemple, utiliser les systèmes informatiques pour accéder de façon non autorisée aux fichiers confidentiels et les copier sur un support amovible[6, 7, 8, 9]. Malgré leur popularité, **les SDI hôtes sont insuffisants,** car plus de la moitié des cas d'exfiltration des données se produit sur les réseaux. En effet, les acteurs internes utilisent principalement leur adresse courriel professionnelle pour envoyer les données confidentielles de l'entreprise à l'extérieur du réseau[9].

Les SDI s'appuient également sur deux techniques principales permettant la détection d'une intrusion. **La détection fondée sur les signatures** s'appuie sur des techniques de correspondance (d'où la notion de « signatures ») de modèles pour déceler une menace[10]. Les SDI s'appuyant sur cette technique sont simples à implanter, car ils ne font que comparer les données avec la base de données des signatures[11]. Par exemple, un SDI peut détecter l'exfiltration des données confidentielles en signalant les instances où l'expéditeur envoie des fichiers joints dont la taille dépasse un seuil prédéterminé par les concepteurs[12]. Or, ces indicateurs ne sont pas infaillibles aux faux positifs : un employé pourrait très bien envoyer légitimement un grand nombre de fichiers à l'externe. En outre, les SDI fondés sur les signatures ne permettent que de repérer les menaces connues et leur efficacité dépend d'une mise à jour constante de la base de données des signatures[11, 13].

Cette technique de détection est notamment inefficace contre les vulnérabilités « zero-days », c'est-à-dire les vulnérabilités méconnues de tous à l'exception des attaquants[14].

La détection fondée sur les anomalies implique de former le SDI à reconnaître les activités habituelles au sein d'un système ou d'un réseau quelconque. Il peut ensuite signaler tout événement informatique inhabituel. Par exemple, des chercheurs [15] ont conçu un algorithme qui évalue et détecte les anomalies selon la fréquence de connexion habituelle de l'usager, le nombre de courriels envoyés et reçus, et la destination ainsi que la provenance des courriels en question.

Les organisations optent plus souvent pour la détection fondée sur les anomalies, car elle permet de repérer les attaques auparavant inconnues[2]. En revanche, elle est susceptible d'émettre de faux positifs, notamment dans les milieux de travail dynamiques où les comportements au sein du système ou du réseau informatique varient selon les exigences des divers projets entrepreneuriaux[16]. La rotation des employés dans le milieu de travail peut aussi déclencher des changements dans les activités habituelles de l'organisation[6]. De même, il est possible que l'algorithme ait considéré des opérations malveillantes comme étant des activités habituelles durant la phase d'apprentissage du SDI[11]. Les concepteurs se doivent de réinitialiser le processus, ou encore installer un algorithme dynamique qui s'ajuste aux changements des événements informatiques[6] (voir tableau en annexe pour un résumé des avantages et inconvénients des deux techniques).

La majorité des activités informatiques sont bénignes[17] ce qui explique que certaines études ont tenté d'intégrer des indicateurs comportementaux et psychologiques supplémentaires dans les SDI afin de réduire le taux de faux positifs[6]. Cette approche suggère que les acteurs internes malveillants présentent certaines caractéristiques personnelles distinctes,

ce qui permettrait aux analystes de cybersécurité d'effectuer un premier tri des signalements des SDI et se focaliser sur les individus à risque[18, 19]. Des chercheurs ont développé un algorithme pour prédire le niveau de risque posé par un employé à l'aide de douze précurseurs psychosociaux de la menace interne[20]. Dans une autre étude, des chercheurs ont quant à eux construit un outil qui déduit les traits de personnalité propices à la menace interne — notamment le narcissisme, le machiavélisme et la recherche d'émotions fortes — à partir du contenu des sites internet régulièrement visités par les individus étudiés[19]. Enfin, dans une autre étude[21] des chercheurs ont conçu un modèle de détection des comportements de rejet d'autorité à partir des commentaires émis sur YouTube concernant la police, argumentant que ce trait est associé à la menace interne.

D'autres SDI utilisent de données provenant des ressources humaines[6, 12] tels que ceux s'appuyant sur les comptes d'utilisateur des employés expirants sous 30 jours, car il a été mis en avant qu'une majorité des cas d'incidents de menace interne aient impliqué des employés ayant reçu un préavis de licenciement et que les attaques ont eu lieu entre la remise du préavis et la fin d'emploi. Il est important de souligner que les données psychosociales sont utilisées afin de compléter les SDI pour faciliter la gestion des risques et ne peuvent indiquer à elles seules la présence d'un acteur interne malveillant[22] d'autant plus que la menace interne représente une infime partie de la main d'œuvre d'une organisation[23] (pour de plus amples informations sur les facteurs psychosociaux de la menace interne, voir la fiche synthèse vol. 2 num. 5).

L'effet dissuasif des SDI

Les SDI reposent sur le principe de dissuasion de la menace. Les organisations espèrent augmenter la certitude de détection par l'entremise des SDI et ainsi dissuader la violation des politiques de sécurité[5]. Il n'existe pas d'études sur l'effet dissuasif des SDI, mais celles portant sur les technologies de surveillance numérique (surveillance de la navigation web, surveillance des activités sur le réseau, audits de sécurité, etc.) contiennent des éléments pertinents qui pourraient être appliqués aux SDI. Une étude a d'ailleurs[24] montré que la surveillance numérique accroît les perceptions de certitude et de sévérité de la sanction chez les employés. D'autres études démontrent également que la perception de certitude de la punition engendre l'obéissance aux règles de sécurité[25, 26]. En revanche, selon cette étude, la perception de certitude de la sanction affecte principalement les employés qui partagent les valeurs de l'organisation, car ils sont plus sensibles à la réputation de l'organisation[24]. De plus, les technologies de la surveillance avivent les perceptions de sévérité de la punition parce qu'elles facilitent la détection de violations menant à de sévères mesures disciplinaires (comme le congédiement). Une autre étude montre quant à elle que la surveillance numérique, à elle seule, a un effet dissuasif plus important que les politiques organisationnelles de cybersécurité[25].

L'effet pervers des technologies de surveillance

Bien que les capacités de détection des SDI semblent à première vue maintenir un certain effet dissuasif sur la menace interne, une implantation purement unidirectionnelle risque d'entraîner des conséquences inattendues et exacerber la menace interne au sein d'une organisation. Autrement dit, la volonté dissuasive néglige de prendre en compte les valeurs morales des employés et comment celles-ci peuvent entrer en conflit avec la certitude et la sévérité des sanctions. La perception de la sévérité de la sanction réduit le climat de confiance dans le milieu de travail et exacerbe subséquemment la désobéissance aux règles de conformité, même chez les personnes qui s'étaient auparavant identifiées aux valeurs de l'entreprise[27]. Des auteurs argumentent d'ailleurs que la surveillance numérique restreint l'engagement organisationnel des employés[28]. Plus spécifiquement, les actions altruistes qui dépassent les obligations formelles d'un employé à l'intérieur d'une organisation diminuent en réponse à la surveillance[29, 30]. Une étude montre comment

la surveillance électronique circonscrit chez les travailleurs la perception d'un lien strictement économique et utilitariste avec leur employeur : ces employés vont bel et bien remplir leurs fonctions formelles en échange de rémunération, mais ils ne verront pas d'incitatifs à prendre d'initiative ou à innover en faveur de l'organisation[30].

La théorie de la réactance psychologique postule que chaque personne possède un certain niveau de liberté individuelle dans son quotidien et que sa mise en danger engendre la réactance[31]. La réactance consiste en une réponse affective négative qui motive la résistance contre la menace en question (dans ce cas-ci les technologies de surveillance) en vue de préserver le sentiment de liberté individuelle. Ainsi, la déviance dans le milieu de travail augmente lorsque les entreprises qui prônent l'autonomie des employés introduisent simultanément des mesures de surveillance[33] parce que les travailleurs deviennent incertains du niveau de contrôle qu'ils détiennent dans le cadre de leurs fonctions. Les mesures de surveillance entravent cette liberté, poussant les employés à se rebeller dans le but de reprendre le contrôle d'une certaine autonomie. L'implantation des SDI afin d'assurer le respect des règles de conformité, risque donc de contrarier les employés souhaitant accomplir leurs tâches de leur propre chef et leur inspirer de la réactance.

Des chercheurs montrent pour leur part que donner une perception d'autonomie élimine les attitudes négatives à l'égard de la surveillance électronique — comme l'atteinte à la vie privée ou le sentiment de méfiance de l'organisation envers ses employés — propices à la déviance dans le milieu de travail[34]. Selon cette étude, donner aux employés un sentiment de contrôle permet d'absorber la réactance. Ainsi, l'autonomie n'entre pas en conflit avec la surveillance[33]. Les conclusions divergentes des études peuvent s'expliquer par leur échantillonnage différent (population étudiante[33] versus employés d'entreprises[34]).

Un autre enjeu en lien les technologies de surveillance concerne la protection de la vie privée. Selon la théorie de la gestion de la confidentialité des communications, les individus estiment détenir un droit à la vie privée, peu importe le contexte légal[35]. Ils établissent des frontières dans lesquelles se trouvent les informations qu'ils choisissent de divulguer. Ces frontières sont renégociées selon le contexte dans lequel se trouvent ces personnes. Les employés s'attendent donc généralement à partiellement concéder des incursions au sein de ces « frontières » à des fins de surveillance[35]. Des complications peuvent toutefois survenir lorsque l'organisation viole les frontières initialement négociées de manière plus ou moins explicite[35, 36], ce qui engendre un climat de méfiance[36]. Ainsi, recueillir des informations non reliées à l'emploi risque de provoquer des tensions[37].

Des chercheurs montrent pour leur part que les employés prédisposés à la réactance perçoivent la surveillance électronique comme impliquant une plus grande atteinte à leur vie privée et ceux-ci auront davantage tendance à désobéir aux politiques organisationnelles de cybersécurité pour regagner leur liberté[38]. De même, l'orientation éthique des travailleurs modère la réaction à l'égard des technologies de surveillance[39]. Les individus prédisposés à l'utilitarisme tolèrent leur usage malgré les atteintes qu'elles peuvent porter à la vie privée s'ils croient qu'elles sont indispensables à la bonne gestion de l'organisation. Ces atteintes préoccupent également assez peu les formalistes, c'est-à-dire les personnes qui croient que l'obéissance aux règles va de pair avec la conduite morale.

Limites et recommandations

Les SDI représentent une piste novatrice pour détecter la menace interne, mais les études portant sur leur efficacité ne sont pas concluantes. Dans la plupart des cas, les SDI étudiés n'ont pu être testés qu'une seule fois, car les auteurs ont omis de fournir des précisions sur le processus de construction de l'algorithme et sa performance[2]. Par ailleurs, les expérimentations s'appuient sur des attaques simulées, car l'accès à des bases de données réelles s'avère difficile[14].

Il importe donc aux praticiens de reconnaître que les résultats risquent d'être différents sur le terrain.

En outre, certaines études portant plus spécifiquement sur les données psychosociales risquent d'apporter un portrait erroné de la menace interne en raison de l'opérationnalisation des facteurs de risque. Par exemple, le mépris pour l'autorité est un facteur de risque à la menace interne certes[20], mais le jauger à partir des messages concernant les forces de l'ordre sur les médias sociaux[21] devient problématique si le contexte social élargi est mis de côté. D'autre part, les études ne traitent pas suffisamment des répercussions négatives inattendues possibles liées à la réactance et à la résistance subséquente aux politiques de sécurité.

L'étude du facteur humain de la menace interne permet de mieux équiper les organisations afin de faire face à ce type d'enjeu :

- À l'aide de mécanismes de rétroaction, prendre en compte les sentiments des employés à l'égard des informations capturées par les SDI. Les recherches indiquent que cette façon de procéder favorise le sentiment de consultation et d'agentivité dans la conception des procédés organisationnels[29]— et qu'elle diminue les perceptions d'atteinte à la vie privée lorsque les données psychosociales sont considérées[37, 40]. Agir de la sorte évite aussi l'asymétrie entre les actions de l'organisation et les attentes des employés[35].

- Offrir plus d'autonomie aux employés quant à la façon d'effectuer leurs tâches quotidiennes. Cette démarche permet d'augmenter leurs sentiments de contrôle et minimisera les effets négatifs des technologies de surveillance[34].

- Justifier l'implantation de la surveillance électronique et concevoir le message de façon à incorporer l'ensemble des orientations éthiques des employés[39]. Plus précisément, les gestionnaires devraient mettre l'accent sur l'importance des SDI dans le maintien du bon fonctionnement des opérations pour satisfaire les utilitaristes.

En somme, les organisations mettant en place des SDI doivent faire attention de ne pas sacrifier la solidarité et l'engagement au sein du milieu de travail en vue de contrecarrer la menace interne — les valeurs auxquelles souscrivent les employés et qui influencent leur conformité aux règles, leur productivité et leur sens de l'innovation supplantent les effets de la dissuasion.

Références

[1] Bellovin, S. M. (2008). The insider attack problem: nature and scope. Dans S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith et S. Sinclair (dir.), *Insider Attack and Cyber Security: Beyond the Hacker* (p. 5-16). Boston, MA : Springer US.

[2] Gheyas, I. A. et Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Analytics, *1*(1), 1-29.

[3] Statistics Canada. (2018). Statistics Canada - SERENE-RISC. https://www.serene-risc.ca/en/statistics-canada

[4] Liu, A., Martin, C., Hetherington, T. et Matzner, S. (2005). A comparison of system call feature representations for insider threat detection. Communication présentée au Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop (p. 340-347).

[5] Scarfone, K. et Mell, P. (2012). Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) (p. 1-111). ÉU : National Institute of Standards and Technology.

[6] Liu, L., De Vel, O., Han, Q.-L., Zhang, J. et Xiang, Y. (2018). Detecting and preventing cyber insider threats: A survey. IEEE Communications Surveys Tutorials, *20*(2), 1397-1417.

[7] Kozushko, H. (2003). Intrusion detection: host-based and network-based intrusion detection systems, 1-23.

[8] Han, K., Mun, H., Yeun, C. Y. et Kim, K. (s. d.). Design of intrusion detection system preventing insider attack, 419-430.

[9] Cappelli, D., Moore, A. et Trzeciak, R. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud). Addison-Wesley.

[10] Khraisat, A., Gondal, I., Vamplew, P. et Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, *2*(1), 1-22.

[11] Rao, U. H. et Nayak, U. (2014). Intrusion detection and prevention systems. Dans U. H. Rao et U. Nayak (dir.), *The InfoSec Handbook: An Introduction to Information Security* (p. 225-243). Berkeley, CA : Apress.

[12] Hanley, M. et Montelibano, J. (2011). Insider threat control: using centralized logging to detect data exfiltration near insider termination, 1-23.

[13] Penta Security. (2016). The benefits of using signature-less detection technology. Penta Security Systems Inc.

[14] Azeez, N. A., Bada, T. M., Misra, S., Adewumi, A., Van der Vyver, C. et Ahuja, R. (2020). Intrusion detection and prevention systems: an updated review. N. Sharma, A. Chakrabarti et V. E. Balas (dir.), Communication présentée au Data Management, Analytics and Innovation, Singapore (p. 685-696).

[15] Kim, J., Park, M., Kim, H., Cho, S. et Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences*, *9*(19), 1-23.

[16] Chae, Y., Katenka, N. et DiPippo, L. (2019). An adaptive threshold method for anomaly-based intrusion detection systems. 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA) (p. 1-4). 10.1109/NCA.2019.8935045

[17] Azaria, A., Richardson, A., Kraus, S. et Subrahmanian, V. S. (2014). Behavioral analysis of insider threat: a survey and bootstrapped prediction in imbalanced data. *IEEE Transactions on Computational Social Systems*, *1*(2), 135-155.

[18] Liang, N. (Peter), Biros, D. P. et Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, *33*(2), 361-392.

[19] Alahmadi, B. A., Legg, P. A. et Nurse, J. R. C. (2015). Using Internet activity profiling for insider-threat detection.

[20] Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C. et Hohimer, R. E. (2012). Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats. Communication présentée au 2012 45th Hawaii International Conference on System Sciences (p. 2392-2401).

[21] Kandias, M., Stavrou, V., Bozovic, N. et Gritzalis, D. (2013). Proactive insider threat detection through social media: the YouTube case. Communication présentée au Proceedings of the 12th Workshop on privacy in the electronic society, Berlin, Germany (p. 261–266). 10.1145/2517840.2517865

[22] Legg, P. A., Moffat, N., Nurse, J. R. C., Happa, J., Agrafiotis, I., Goldsmith, M. et Creese, S. (2013). Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *4*(4), 20-37.

[23] Pfleeger, C. P. (2008). Reflections on the insider threat. Dans S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith et S. Sinclair (dir.), *Insider Attack and Cyber Security: Beyond the Hacker* (p. 5-16). Boston, MA : Springer US.

[24] D'Arcy, J., Hovav, A. et Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), 79-98.

[25] Herath, T. et Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

[26] Kuo, K.-M., Talley, P. C. et Cheng, T.-J. (2019). Deterrence approach on the compliance with electronic medical records privacy policy: the moderating role of computer monitoring. *BMC Medical Informatics and Decision Making*, *19*(1), 1-12.

[27] Li, H., Zhang, J. et Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, *48*(4), 635-645.

[28] Tabak, F. et Smith, W. P. (2005). Privacy and electronic monitoring in the workplace: a model of managerial cognition and relational trust development. *Employee Responsibilities and Rights Journal*, *17*(3), 173-189.

[29] Jahangir, N., Akbar, M. M. et Haq, M. (2004). Organizational citizenship behavior: Its nature and antecedents. *BRAC University Journal*, *1*(2), 75-85.

[30] Jiang, H., Siponen, M. et Tsohou, A. (2019). A field experiment for understanding the unintended impact of internet monitoring on employees: policy satisfaction, organizational citizenship behaviour and work motivation.

[31] Lowry, P. B. et Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, [25](5), 433-463.

[32] Lawrence, T. B. et Robinson, S. L. (2007). Ain't misbehavin: Workplace deviance as organizational resistance. *Journal of Management*, *33*(3),

[33] Jensen, J. M. et Raver, J. L. (2012). When self-management and surveillance collide: Consequences for employees' organizational citizenship and counterproductive work behaviors. *Group & Organization Management*, *37*(3), 308-346. 10.1177/1059601112445804

[34] Martin, A. J., Wellen, J. M. et Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. *The International Journal of Human Resource Management*, *27*(21), 2635-2651.

[35] Watkins A., M., Coopman, S. J., Hart, J. L. et Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. Management Communication Quarterly, 21(2), 172-200. 10.1177/0893318907306033

[36] Snyder, J. L. (2010). E-mail privacy in the workplace: a boundary regulation perspective. The Journal of Business Communication, 47(3), 266-294. 10.1177/0021943610369783

[37] Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. Journal of Applied Psychology, 86(4), 797-804. 10.1037/0021-9010.86.4.797

[38] Yost, A. B., Behrend, T. S., Howardson, G., Badger Darrow, J. et Jensen, J. M. (2019). Reactance to electronic surveillance: A test of antecedents and outcomes. *Journal of Business and Psychology*, *34*(1), 71-86.

[39] Alder, G. S., Schminke, M., Noel, T. W. et Kuenzi, M. (2008). Employee reactions to internet monitoring: the moderating role of ethical orientation. *Journal of Business Ethics*, *80*(3), 481-498.

[40] Posey, C., Bennett, R., Roberts, T. et Lowry, P. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, *7*, 24-47.