ESTUDO DE CASO MONITORAMENTO DE ATIVOS DE REDES: DIFICULDADE DE MONITORAMENTO DE USUÁRIOS

CLAUDINEI RIBEIRO MENDONÇA, FELLIPE DE LIMA MATHIAS, KEIJI NAKAMURA, LUAN MARIANI PASSOS, RENATO ARAÚJO CRUZ, SORAIA CASTELLANO, VICENTE TRUDES F. G. FREITAS, WESLLEY M. DA SILVA, ELINEY SABINO

Resumo

Neste artigo, discutiremos as dificuldades existentes no monitoramento de usuários devido a leis impostas assim complicando a vida das empresas que desejam se manterem seguras. Com o monitoramento de atividades, possivelmente os departamentos de uma empresa dificilmente tenham suas informações ou sofram algum tipo de ataque, desta forma sentem-se seguras em salvar arquivos confidenciais em seus computadores.

Palavras chaves: Redes de Computadores, Monitoramento, TI, Segurança da Informação

Introdução

O objetivo deste artigo, visa discutir a dificuldade do monitoramento de funcionários, que segundo a legislação brasileira (LEI Nº 12.965, DE 23 DE ABRIL DE 2014, Art. 3º) é ilegal e imoral para a empresa.

Com isso, iremos abordar as possíveis soluções para alguns dos problemas que empresas vem sofrendo, tais como, vazamento de informações, invasões de *hackers* ou *crakers*, entre outros.

O monitoramento é necessariamente algo realizado, 24 horas x 7 dias por semana. Mas sempre que falamos de monitoramento pensaremos na privacidade do usuário, e isso é um dos motivos, dos quais apresentaremos algumas sugestões.

A dificuldade encontrada hoje em dia é justamente para que o monitoramento mantenha a privacidade de seus usuários intacta e a segurança de rede da empresa segura é essencial.

O monitoramento das atividades dos usuários se torna importante por conta da segurança, privacidade e integridade de empresas e de seus usuários que tem acesso as suas respectivas redes. Empresas de pequeno e médio porte estão aderindo ao monitoramento como forma de solução para proteger seus usuários e evitar que suas informações sejam vazadas.

Manter o monitoramento das atividades dos usuários é de extrema importância para que a empresa tenha as suas informações preservadas. A importância de se monitorar é justamente para que atitudes suspeitas dos usuários sejam investigadas pelo setor de Tecnologia da Informação (TI) para continuar mantendo a segurança e integridade da empresa.

Afirmam Benini e Daibert (2011, s/n), como é impossível evitar os problemas na rede, a melhor forma de resolver o impacto causado é através do monitoramento.

Monitoramento e suas ações

Conforme Soares (2013), Redes de Computadores, o nome é sobre a interconexão de comunicações por diversos meios com um único objetivo, trocar informações e outros recursos. Isso é chamado de estações de trabalho ou dispositivos de rede. Exemplo, se existem dois computadores em uma casa ou estação de trabalho eles não se comunicam por si próprio mas por meio de cabos interligados, podem fazer com que eles comecem a ter acesso a internet, desta forma teremos uma rede. A partir daí surgiram diversos conceitos sobre redes de computadores, como protocolo *Transmission Control Protocol/* Internet Protocol *(*TCP/IP), transferência de pacote de dados, e entre outros, todos relacionados ao nascimento da internet. Após isso, propósitos acadêmicos e trabalhos de pesquisas em diversas campus de universidades eram sobre redes de computadores. Hoje em dia, temos interconexões entre computadores em diversos lugares do mundo que nos permite a transferência de pacote de dados, comunicação entre usuários, tanto quando estão na internet ou na televisão.

Segundo Oliveira (2017), atualmente podemos enviar e-mails e mensagens através de qualquer dispositivo móveis com acesso à internet, como um *tablet ou smartphone*. Porém, o crescimento tem seu lado negativo, e a cada dia surgem problemas que atrapalham usuários como espionagens, piratarias, roubos de identidades (*phishing*), entre outros mais graves como racismo, pornografia e sexo. Atualmente temos diversos tipos de redes, das mais longas ou até mesmo a da sua casa, tais como;

> Redes Pessoais (*Personal Area Networks* – PAN) – se comunicam a 1 metro de distância. Ex.: Redes Bluetooth; Redes Locais (*Local Area Networks* – LAN) – redes em que a distância varia de 10m a 1km. Pode ser uma sala, um prédio ou um campus de universidade; Redes Metropolitanas (*Metropolitan Area Network* – MAN) – quando a distância dos equipamentos conectados à uma rede atinge áreas metropolitanas, cerca de 10km. Ex.: TV à cabo; Redes a

> Longas Distâncias (*Wide Area Network* – WAN) – rede que faz a cobertura de uma grande área geográfica, geralmente, um país, cerca de 100 km; Redes Interligadas (Interconexão de WANs) – são redes espalhadas pelo mundo podendo ser interconectadas a outras redes, capazes de atingirem distâncias bem maiores, como um continente ou o planeta. Ex.: Internet; Rede sem Fio ou Internet sem Fio (*Wireless Local Area Network* – WLAN) – rede capaz de conectar dispositivos eletrônicos próximos, sem a utilização de cabeamento. Além dessa, existe também a (*Wireless Metropolitan Area Network*) WMAN, uma rede sem fio para área metropolitana e *Wireless Wide Area Network (*WWAN*)*, rede sem fio para grandes distâncias. (OLIVEIRA, 2017, s/n)

Para Sousa (2010), A interligação de várias redes é feita por meios de comunicação, como as Linhas Privativas (LP), redes públicas e roteadores, que são ligadas entre si e compartilham os dados de acordo com o endereço de destino de rede. As redes e seus equipamentos também devem ser planejados e construídos baseados em padrões de comunicações, para assim permitir a comunicação entre diferentes sistemas operacionais e computadores.

Afirma Morimoto (2008), as redes atualmente cumprem sua função como uma opção de compartilhar recursos entre diversos computadores, permitindo que você tenha acesso aos dispositivos como use impressoras, *Compact Disc Read-Only Memory (Disco Compacto de Memória Apenas de Leitura*) CD-ROMs entre outros dispositivos e rede de aplicativos.

De acordo com Tanebaum (2014), nas empresas atualmente existem um grande número significativo de computadores. Os mesmos são usados pelos seus colaboradores atribuídos para sua função especifica, tais como, escrever documentos, elaborar folhas de pagamentos, contratos, entre outras funções. No início, alguns destes computadores pode trabalhar isoladamente, mas em algum momento terão de ser conectados uns aos outros, uma gerência de rede também será necessária para que funcionem de forma coerente.

Conforme Jacques (2015), sobre softwares de monitoramento nos computadores das escolas tem como função colaborar com os professores para que as aulas não percam seu foco, além disso o software acabou dando diversas ideias, e até mesmo colaborou para que os professores pudessem aplicar sua aula até mesmo à distância. Quando alguns professores foram perguntados disseram que faltam ferramentas

que pudessem auxiliar o professor e o aluno para que tivesse uma aula mais produtiva quando estão nos computadores da escola, pois falta foco aos alunos quando estão nos computadores com diversos aplicativos à disposição. Até que implementaram um sistema multi-agente como colaboração para que o professor tenha auxilio e possa ter uma avaliação melhor dos seus alunos e da sua aula ou curso. Com isso podemos usar de exemplos para a aplicar da mesma forma empresas, porém nunca usando daqueles dados que são particulares e privados de seus usuários, para que seus chefes e cargos maiores tirem proveitos sobre essas informações pois assim estariam tirando dos seus funcionários direitos a privacidade.

> Monitorar é controlar, supervisionar por diversos meios, fatores ligados à saúde, segurança, meio ambiente, produção, desempenho e outros. O monitoramento pode se manifestar de várias formas no ambiente de trabalho com a utilização de câmeras, rastreamento de sites e e-mails, rastreamento via satélite, escutas telefônicas, revistas pessoais, monitoramento de substâncias prejudiciais à saúde e outros. (Silva, 2007 s/n),

Segundo Barros (2006, s/n), o legislador brasileiro nunca proibiu a fiscalização e controle por meios de aparelhos audiovisuais, por ser algo que veio devido ao avanço da tecnologia e pode ser usado em uma ferramenta valiosa para avaliar a conduta de um funcionário.

> (...) a vídeo vigilância em estudo deve obedecer a certos princípios gerais que também são comuns a outros tipos de monitoração (*e-mail e sites*). Tais princípios são encontrados no grupo do artigo 29 da diretiva 95/46 do Conselho da Europa, são eles: necessidade, finalidade, transparência, legitimidade, proporcionalidade, rigor e retenção de dados e, por final, segurança. (Barros, 2006, s/n)

Para Pantaleão (2016), para que o empregador não tenha possíveis problemas trabalhistas com a utilização errada destes recursos, há algumas sugestões, tais como;

- Manter o empregado informado que existe uma forma de monitoramento assim que for contratado;

- Não instalar câmeras em lugares que tiram a privacidade dos funcionários como (banheiros, vestiários, salas individuais);
- Não focar em apenas uma área ou pessoa, pois o monitoramento pode ser alvo de discriminação por parte da empresa;
- Nunca disponibilize imagens ou áudios a terceiros. Informações do monitoramento é somente ao pessoal responsável, e quando necessário, ás autoridades.

Segundo Pantaleão (2016), a tecnologia atualmente nos traz diversas ferramentas como softwares para monitoramento em estações de trabalho, para execução de atividades de rotinas e que são monitoradas. Outro ponto relativo refere-se à proibição de acesso pela internet de determinados *sites*. Novamente, como os equipamentos e *softwares* pertencem à empresa, qualquer prejuízo ocasionado ao mal-uso dos computadores será de total responsabilidade do empregador. Principais precauções que devem ser adotadas:

- Informar ao funcionário que está sendo monitorado o seu computador;
- Deixar claro quais sites poderão ser acessados, determinar a proibição ao acesso livre da internet em horários de intervalo.

Afirma Costa (2016), com o monitoramento, caso o funcionário seja pego em flagrante fazendo algo proibido na empresa, ele deve ser demitido por justa causa, fica a critério do empregador. Em casos mais leves como acesso as redes sociais, isso pode levar a uma suspenção ou advertência, ao chegar a três advertências o funcionário deve ser demitido por justa causa. Caso for pego fazendo algo mais grave, tais como acessando pornografia infantil, pirataria, divulgação de informações, entre outros, deve ser conduzido à delegacia e ser demitido por justa acusa, pois se o empregador acobertar estes crimes, pode ser indiciado da mesma forma. De olho nisso e como os computadores vem sendo a principal ferramenta de trabalho em muitas empresas, desenvolvedoras de softwares que servem como forma de monitoramento vêm investindo ao decorrer dos anos e deve ser mais comum no futuro próximo.

Uma vez provado o fato, as provas podem ser usadas para justa causa, já que as imagens é uma forma legal e um dos meios utilizados pela empresa para sua defesa contra eventuais reclamatórias trabalhistas para sustentas a justa causa. Não pode se deixar passar a observação destes requisitos necessários, pois podem custar muito caro ao empregador, para Pantaleão (2016).

> Às vezes é melhor demitir um empregado sem justa causa por um suposto roubo (onde há apenas uma suspeita) do que usar de

> artifícios ilegais e ter que indenizá-lo 20 ou 30 vezes mais do que o valor do objeto/informação que supostamente tenha roubado. (Pantaleão, 2016, s/n)

Segundo Martins (2015), as pessoas costumam acessar, no local de trabalho, redes sociais, sites de bate papo, e-mail pessoal, até mesmo sites de pornografia, com isso os empregadores devem ficar atentos e evitar estas práticas, visto que elas podem trazer prejuízos para empresa. E o lado do funcionário é que pode perder os direitos trabalhistas, como o seguro desemprego, aviso prévio, 13º salário, e o saque do Fundo de Garantia do Tempo de Serviço (FGTS), caso venha ser pego e muito provavelmente demitido por justa causa.

Considerações Finais

Para Luan, A importância do tema monitoramento de redes se dá pelo crescimento do número de usuários com a capacidade de danificar um sistema ou até mesmo efetuar vazamento de dados. Em uma época que muitos setores da sociedade utilizam a informática e realizam a troca de informação digitalmente a importância e o valor de dados vem crescido abundantemente, assim tendo que ser mantida a devida segurança, não só para empresas, mas também para usuários. Entretanto, não só usuários com más intenções podem danificar um sistema ou vazar dados, existe diversas possibilidades que devem ser levadas em conta, dando assim mais importância para a realização do controle e monitoramento de usuários na rede.

Para Felipe, o monitoramento é grande problemas nas empresas atualmente com funcionários que não respeitam o próprio ambiente de trabalho. As empresas acabam entrando em conflito e se fazendo a seguinte pergunta: "até que ponto pode chegar o monitoramento dos usuários em prol da segurança"?

Para Claudinei, o monitoramento é algo necessário dentro de uma empresa, pela falta de responsabilidade dos usuários de rede, pois acessam conteúdos indevidos. Apesar do monitoramento, usuários sempre acham meios de dribla-los com softwares ou manhas. Nos dias atuais existem diversos tipos de monitoramento para empresas se preservarem. Infelizmente usuários não sabem usar os acessos que as empresas disponibilizam para eles.

Para Wesley, é preciso aprimorar a segurança nas redes e melhorar a qualidade de monitoramento do mesmo, para que assim, tenha um bom funcionamento nas redes da empresa e evitar possíveis ataques no sistema da mesma e não prejudicar tanto ela como os colaboradores.

Para Vicente, o monitoramento é uma forma de se aproveitar mais o tempo em serviço e ver quais funcionários estão aplicados em realmente exercer seu trabalho da forma correta e no tempo correto. Sobre a privacidade do usuário, deve ser mantida e só usada em casos extremos.

Referências bibliográficas

Barros Alice M., http://www.uel.br/revistas/uel/index.php/direitopub/ Acessado em 18/05/2017

Costa, Vagner., http://www.artigos.com/artigos/21479-empresa-pode-monitorar-funcionarios Acessado em 18/05/2017

Jaques, Patrícia E., https://www.researchgate.net/profile/Patricia_Jaques/

Acessado em 05/05/2017

Lautré, Evelyne, http://revista.ibict.br/ciinf/article/view/447 Acessado em 05/05/2017

Martins, Erica Verissimo,. ., <https://ericaverissimoadv.jusbrasil.com.br/artigos/112298373/monitoramento-de-meios-eletronicos-no-ambiente-de-trabalho-e-suas-consequencias-juridicas> Acessado em 18/05/2017

Morimoto, Carlos E., http://www.hardware.com.br/tutoriais/historia-redes/

Acessado em 28/04/2017

Oliveira, Felipe S., http://blog.unipe.br/graduacao/conheca-tudo-sobre-a-historia-das-redes-de-computadores Acessado em 28/04/2017

Presidência da República do Brasil, Casa Civil, Subchefia para Assuntos Jurídicos: LEI Nº 12.965, DE 23 DE ABRIL DE 2014. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, Acessado em 28/04/2017

Pantaleão, Sergio F., www.guiatrabalhista.com.br/monitoramento_empregados/

Acessado em 18/05/2017

Soares , Ari Clayton. http://ariclayton.blogspot.com.br/2013/02/

Acessado em 28/04/2017

Tanenbaum, Andrew S., Redes de Computadores, 5ª Edição, Editora PEARSON , 2014.