ETEC DE SAPOPEMBA

INTELIGÊNCIA ESTRATÉGICA E SEGURANÇA CORPORATIVA NA GESTÃO DE PESSOAS

Weverton Antonio Carlos Niza

RESUMO

Agressões, ataques, fraudes, paralisações, sabotagens, danos e riscos operacionais em sua maioria são incrementados dentro das organizações.

Esse conjunto inclui desde os insatisfeitos e desajustados, passando por pessoas cooptadas ou infiltradas por concorrentes, pessoas que representam o maior risco que o sistema pode enfrentar. Presentemente já se fala, nos ‘’web mercenários’’, criminosos contratados para invadir, suprir ou alterar dados em sistema de concorrentes. As necessidades que se pretende atingir, sem perder de vista propostas de integração horizontal na área de segurança, bem como, a concepção de que existe a necessidade de ações de sensibilização, supervisão e monitoramento de pessoas na organização que possam pôr em risco a segurança das informações. Os perigos e riscos são inerentes à atividade empresarial. Nada é mais arriscado do que colocar seu capital humano sujeito a normas externas e ações humanas diversas.

Publicação segundo o autor do artigo Segurança Empresarial - Riscos na segurança das informações & dados de Carlos Paiva 27 de dezembro de 2013, São Paulo, e o artigo Riscos na segurança das informações & dados- www.administradores.com.br

Palavras-chave: Inteligência, Segurança Corporativa, Recursos Humanos.

INTRODUÇÃO

Muito se tem discutido, recentemente, acerca da inteligência estratégica em relação à segurança corporativa, para um ótimo desempenho da empresa. Na modernidade, atualmente em todos os quesitos, a área mais desejada por

todos, é a área de trabalho. As empresas e consultorias de recursos humanos dizem que há uma escassez de profissionais qualificados para o mercado de trabalho.

Consequentemente, as concorrências entre as empresas buscam estar atentos aos melhores profissionais, além de cada vez mais o mercado estar mais exigente. Atualmente o profissional busca por mais formações e treinamentos, logo, agrega mais conhecimento, com participações em networks, se tornando alvo de um mercado carente dele. Então, empresas se atualizam e mudam suas formas que atualmente são de colaboradores de RH, para o recrutamento e seleção nas empresas.

Entender a importância do primeiro filtro (seleção do currículo), criar banco de dados que aderem aos requisitos para próxima etapa de processo aplicando testes relacionado que a área competente exija, é fundamental para avaliação se o candidato adere ao perfil. Pesquisa social avalia candidatos através de sua carteira de trabalho em relação à veracidade do currículo.

Entrar em contato com as empresas cujo as quais os candidatos já trabalharam, ligando informações e identificando a veracidade das informações, analisando junto ao departamento visando evitar erros após a contratação. Analisar criteriosamente registros na carteira de trabalho, para averiguar uma possível fraude, adulteração, ou falsificação, diminuindo riscos. Posterior a pesquisa social, em caso de aprovação, o colaborador deve passar por uma integração monitorada pela inteligência aderindo-o a cultura organizacional adotada.

Mesmo com todos esses filtros, existem pessoas de conhecimentos tecnológicos a serviço do crime. Passam a conhecer a engenharia social, se infiltram nas organizações a serviços de concorrentes para espionar, sabotar, fraudar e, até mesmo praticar atividade terrorista.

Podemos observar e agregar muito mais conhecimento sobre o assunto, analisando na atualidade a guerra entre Rússia e Ucrânia e, a ação do setor de inteligência em relação à informação e dados, também, é possível ver de fato, portas para tais ações com a implantação do 5G. O intuito da inteligência no departamento de recursos humanos é, realizar um filtro particular e mais criterioso em relação à segurança, sabendo criar contramedidas no processo admissional em atividade, ou até mesmo o demissional.

O presente artigo trata da inteligência estratégica e segurança corporativa na gestão de pessoas.

1. SEGURANÇA NO COMBATE A ENGENHARIA SOCIAL

O uso da inteligência competitiva, surgiu na 2° Guerra Mundial, mais especificamente por Estados Unidos e Inglaterra, o conceito foi pela primeira vez além estratégia militar e passou a atuar no campo da ciência, política e criptografia.

Porém, somente na década de 80, com a publicação da obra do Prof° Michael Porter (Harvard Business School) chamada Estratégia Competitiva que o conceito de inteligência competitiva chegou ao mundo dos negócios.

Ambas palavras de origem latin, “inteligência” de “intellegentia” que significa “capacidade de aprender” e a palavra “segurança” que significa “sem preocupações”.

“A Engenharia social faz uso da influência e persuasão para ludibriar pessoas e convencê-las que o engenheiro social possa ser alguém que ele não é, por meio da manipulação.

Como consequência disso, o engenheiro social pode aproveitar-se das oportunidades para obter as informações com ou sem o uso da tecnologia, como defende Mitnick. Kevin D, 2003.

> *“Uma empresa pode ter adquirido melhores tecnologias de segurança que o dinheiro pode comprar. Pode ter treinado seu pessoal tão bem que eles trançam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a adequada do sistema da aplicação das correções da segurança. Esses indivíduos ainda estão completamente vulneráveis. (MITNICK. KEVIN D., 2003, p.21)”*

Observação do consultor de segurança Bruce Schineider, “maior perigo é, colocar pessoas diversificadas em suas instituições”.

Não existe como acabar com os riscos. Porém, estudos ajudam a prevenir, controlando em níveis consideravelmente baixos.

A inteligência e segurança nos recursos humanos, é uma excelente ferramenta na gestão de pessoas, ligando procedimentos de segurança às medidas de prevenção nos controles de candidatos, colaboradores ativos e demitidos.

Através de dados e registros, pode-se procurar por criminosos infiltrados, onde ficam armazenados em computadores todos os registros da corporação, esse é o de maior ameaça.

A segurança das informações, deve ser minuciosa em ambientes humanos onde encontra-se as maiores falhas nas informações de dados.

As inteligências determinam regras que devem ser usadas, colocadas em ação e aderidas aos colaboradores, entendendo que na organização a segurança se encontra sempre alerta.

Colaboradores que estão na zona de conforto, estão aptos as políticas aplicadas pela segurança, porém, precisam ser atualizados em treinamentos para se conscientizarem sobre os riscos e tomem medidas preventivas junto aos recursos humanos, não só em treinamentos, mais como também em auditorias, pontuando colaboradores que não aderem ao comprometimento. O ponto fraco de acesso desses criminosos, é o departamento de recursos humanos, onde a inteligência e segurança tem a missão de filtragem de candidatos.

1.1 IMPORTÂNCIA DA INTELIGÊNCIA E SEGURANÇA NO PROCESSO SELETIVO

Para Mitnick. Kevin D. (2003) a prioridade de todos que trabalham é fazer o trabalho. Sob essa pressão, as práticas de segurança tornam-se obsoletas e são ignoradas. Engenheiros sociais usam isso para praticarem sua arte.

Colaboradores que se encontram na zona de conforto, são resilientes as políticas de segurança, porém, necessitam de atualização em treinamentos para entender os riscos e para que tomem medidas preventivas junto ao departamento de recursos humanos, não só em treinamentos, como em

auditorias, pontuando colaboradores que não aderem ao comprometimento. É no processo seletivo o foco principal de infiltração criminosa.

1.2 BRECHAS NO PROCESSO SELETIVO

”Segundo Kenoby (2017) ter banco de talentos sem qualificação, ter mal planejamento de carreira, ter vagas a serem preenchidas de forma incorretas, triagem mal elaborada, cultura da organização mal definida, engenheiros sociais usam brechas desse tipo para poderem se infiltrarem”.

A pressão no departamento solicitante para preencher a vaga, acaba de certa forma impactando na escolha certa. Informações pessoais do candidato, currículo profissional, cursos e experiências não são o suficiente para decidir sobre o perfil ideal. Para a melhor escolha é preciso realizar testes logo no início.

Uma das falhas mais comuns na seleção é a falta de clareza na apresentação da vaga, com isso, abrem-se brechas para questionamentos de falsos candidatos (engenheiro social), logo os recrutadores acabam sendo manipulados. Do começo ao fim o processo deve estar de acordo com a cultura organizacional, para se obter um melhor filtro dos candidatos.

Triagem mal elaborada pelo RH, para diminuir riscos, deve ser aplicada pela célula da inteligência e segurança, com minuciosos testes comportamentais, pois são os que mais reprovam candidatos.

A cultura da empresa sem uma definição, abre espaço ao engenheiro social, que em seu objetivo de infiltração acaba conhecendo mais a cultura da empresa que o próprio recrutador, atraindo a confiança e manipulando a entrevista.

A pressa para se preencher uma vaga, a realização do relatório do candidato aprovado pelo departamento de RH mal sucedido e com poucas informações, acaba abrindo as portas da empresa para o colaborador criminoso.

2. EXEMPLOS DE ENGENHARIA SOCIAL NA ESPIONAGEM INDUSTRIAL E AS CONTRAMEDIDAS DA INTELIGÊNCIA E SEGURANÇA

Segundo Carvalho, Luciana (2012) relata o furto na Petrobras com relevância à suspeita de espionagem.

O desaparecimento de notebooks e disco rígido da Petrobras em 2008, uma situação de alerta no Brasil. O que poderia ser apenas um furto, foi dado como caso de espionagem, já que nos equipamentos continham informações confidenciais sobre as descobertas do Pré-Sal. A polícia federal descartou a hipótese de espionagem, após deter quatro suspeitos que trabalhavam no terminal portuário do Rio de Janeiro. Equipamentos foram recuperados, garantindo a polícia federal que não houve vazamento das informações.

Por outro lado, trouxe à tona, ocorrências anteriores da mesma espécie.

Em entrevista em 2008, Fernando Siqueira, presidente da Associação Dos Engenheiros Da Petrobras (AEPET), disse que, laptops com informações sigilosas, foram furtados das residências dos engenheiros e outros profissionais indicou suspeitos, porém, as empresas envolvidas conseguiram provar inocência: Galp, British Gás, e a OGX de Eike Batista.

> *"Quando um engenheiro social sabe como as coisas funcionam dentro da empresa-alvo, ele pode usar esse conhecimento para desenvolver a confiança junto aos empregados. As empresas precisam estar preparadas para se desenvolver aos ataques das engenharias sociais vindas de empregados atuais ou ex-empregados, que podem ter motivos de descontentamento. As verificações de histórico podem ser úteis para detectar os candidatos a emprego que tenham uma propensão para esse tipo de comportamento. Mas, na maioria dos casos, é difícil detectar essas pessoas. A única segurança razoável nesses casos é implantar e auditar os procedimentos de verificação de identidade, incluindo o status de emprego da pessoa, antes de divulgar qualquer informação para que qualquer um não se conheça pessoalmente e, portanto, não se sabe se ainda se está na empresa. (MITNICK. KEVIN D., 2003, p.181)"*

As informações contidas nos notebooks, era o que realmente o espião queria, os notebooks foram encontrados em contêineres na zona portuária do Rio de Janeiro com as informações inalteradas, inocentando suspeitos. Porém, esses casos de furtos já haviam ocorrido em outras oportunidades, como relatou Fernando Siqueira, presidente da (AEPET).

Por medida de segurança seria recomendável que esses notebooks, não saíssem da corporação, dificultando furtos e a entrega desses dados por meio de suborno. Outro ponto importante seria a implantação de sistema de segurança da informação nesses equipamentos, de forma intransferível através

de bloqueio e liberação do login pela central de segurança quando for solicitado acesso através de contra senhas geradas aleatoriamente por programas.

O processo seletivo de cada funcionário, seria feito por partes e pessoas diferentes, cada um dos recrutadores teria apenas uma parte das informações, como outra medida de segurança, sendo que todas as informações ficariam apenas com um gestor de alta confiança, logo, esse sim teria as informações completas, dificultando a espionagem.

3. INTELIGÊNCIA E SEGURANÇA MONITORANDO COLABORADORES CRIMINOSOS

Segundo ICTS, metade dos colaboradores tem a tendência de ações irregulares para conquistar seus objetivos. O colaborador criminoso, clona ideias de colegas de trabalho, alteram seus resultados e até pagam suborno.

Empresas são conhecedoras desses fatos, usam tecnologia para monitorar e observar essas pessoas.

Além de vigiar cada passo deles, e contratar empresas no ramo de investigação, se passam por colaboradores como contramedidas nos setores e exercem a mesma função dos suspeitos. Observando o que ele faz.

A contraespionagem entrevista a vida pessoal do suspeito, com profunda discrição, ligando o que eles acreditam que seja apenas uma auditoria.

Dar tal treinamento para o departamento de RH, para essa função investigativa, porém, isso é um papel exclusivo da inteligência e segurança.
“Afinal, quem não deve não teme!”

> *“É incrível como é fácil para o engenheiro social convencer as pessoas a fazerem as coisas com base no modo como se estrutura a solicitação. A tese é acionar uma resposta automática com base nos princípios psicológicos e utilizar os atalhos mentais que as pessoas usam quando o interlocutor é um aliado, analisando a trapaça. (MITNICK. KEVIN D.2003, p.197)”*

Nesses casos têm que ser observadas ações fora do normal desses colaboradores.

3.1. Pertences pessoais

Como um colaborador recebe seu pagamento, e com ele compra roupas finas, possui motos e carros de alto padrão, faz viagens a lugares paradisíacos e frequenta lugares de luxo, se seu pagamento não condiz com tudo isso? Em casos assim a inteligência deve seguir os passos desse colaborador atentamente, monitorar o telefone corporativo de forma que o colaborador não desconfie.

O segredo para o colaborador não cair nessa malha fina é recusar convites e até mesmo brindes de terceiros.

3.2. Consulta SPC e SERASA

Em cargos de alta gestão é indispensável essa pesquisa para saber se esse colaborador possui altas dívidas ao ponto de influenciar suas atividades, tornando-o vulnerável a fraudes ou subornos.

Nesse caso, seria indicado que um profissional da inteligência, usando técnicas psicológicas, dialogasse o máximo possível com esse colaborador para ter ciência do seu cotidiano.

O correto de um colaborador agir é com a verdade e ser verdade quando for questionado.

3.3. Suspeita virtual

Fazer uso de informações confidenciais da empresa para seu benefício é um dos grandes problemas das corporações ao que se trata de espionagem de concorrentes, ou instalam vírus nos computadores.

Por medida de segurança, o ideal é instalar secretamente softwares de segurança para que nenhuma informação seja perdida intencionalmente, ou até mesmo por outros fatores.

Outra questão é investigar colaboradores e redes sociais.

3.4. GPS da honestidade

Instalar programa de rastreamento via GPS em notebooks e celulares para colaboradores que atendem clientes externos, seria uma boa forma de

monitoramento, porém, com falhas se caso esses aparelhos estiverem desligados.

A solução seria usar a central da empresa de segurança para fazer ligações a cada uma hora como contramedidas.

3.5. Fundo fixo “caixinha” monitorada

O departamento de RH tem que ter o controle das verbas depositadas aos colaboradores ao que se diz respeito a benefícios de viagens, hospedagem e alimentação, observando valores usados.

Analisando os valores, os dias, os horários e locais em que foram usados.

Locais usados com maior frequência, gastos que não estão de acordo com o que se foi consumido, pode ser achado como uma possível fraude.

3.6. Convênio médico e farmacêutico

Não se pode saber sobre os problemas de saúde dos colaboradores, pois o acesso é sigiloso devido à ética médica, por outro lado pode-se saber qual o valor gasto e se foi usado o plano de saúde.

O indicado é que tais exames fossem realizados por médicos a serviço da empresa, evitando fraudes.

O RH tem o poder de identificar o colaborador que usou o cartão farmacêutico para compra de medicamentos.

O que deve ser investigado, são gastos de abusos em compra de medicamentos que não condiz com o possível problema de saúde, abrindo suspeitas de fraudes.

4. INTELIGÊNCIA E SEGURANÇA NO PROCESSO DEMISSIONAL

Segundo Sleiman Cristina (2013) O “levar a informação embora” é mais comum do que se imagina e o pior é que os empregados nem sempre têm noção de que cometem uma infração, isso ocorre em qualquer cargo.

> *“Queimar a fonte diz que um atacante queimou a fonte quando permite que uma vítima reconheça que ocorreu um ataque. Após*

> *a vítima tomar conhecimento e notificar os outros empregados ou a direção sobre a tentativa, fica muito difícil explorar a mesma fonte de ataques futuros (MITNICK. KEVIN D.2003, p.45).”*

4.1. Vazamento de informações por ex-colaboradores

As corporações não têm o costume de proteger dados confidenciais nos casos de demissão, por cultura organizacional no Brasil.

Apenas grandes multinacionais possuem normas claras, tomando medidas nesses casos.

Departamento de RH que não se importa tanto com treinamentos e normas, pode haver vazamento de informações, muitas vezes de maneira inocente por parte do colaborador, e o que mais impressiona, é que, isso ocorre da baixa a alta gestão.

Vazar informações é uma ação criminosa, responsabilizando tanto quem levou, quanto quem recebeu.

4.2. O despreparo do RH das corporações para devidas ações de segurança

Não possui o monitoramento de seus colaboradores, sendo assim, acaba facilitando uma ação negativa.

Todo colaborador deve ter ciência da política de segurança da corporação em caso de demissão.

O departamento de RH tem a necessidade de orientação jurídica, para que em processos demissionais por justa causa saiba como proceder com colaboradores criminosos, para que de forma alguma não tome uma “invertida”, sendo processados.

4.3. Neutralizando “invertidas” na demissão

É necessário tornar público as normas e as regras de segurança, cópias das normas e regras de segurança devem ser colocadas em todos os departamentos, em locais visíveis onde todos colaboradores tenham fácil acesso às informações contidas.

Junto às informações, dados jurídicos referentes às informações da corporação e outros de ações criminosas baseadas na ISO 27001 e ISO 27002 (normas internacionais de boa prática).

Publicar cartilhas e folhetos, dar treinamento e feedback constante, para que a gravidade de ações criminosas seja de ciência dos colaboradores, para que saibam que tais ações acarretam em consequências graves.

Considerações Finais

Entende-se que os perigos na corporação são constantes, e o maior de todos os casos, inclusive acidentes, vem através de ações diversas no contexto humano. É impossível mitigar os riscos, porém com inteligência estratégica e segurança corporativa podem sim, ser preventivas e gerenciando em escalas positivas.

A “inteligência estratégica e segurança corporativa na gestão de pessoas” dentro das corporações é uma ferramenta correta de ligação entre os recursos humanos e os colaboradores, não só como um simples departamento nas medidas de segurança, mas atuante conscientização dos colaboradores, tanto em seu desenvolvimento profissional, quanto pessoal.

Friso que atualmente o maior alvo dos colaboradores criminosos, são as informações obtidas através da informatização da corporação através da engenharia social. A inteligência estratégica é um indicador positivo nas movimentações corporativas mitigando riscos.

A inteligência estratégica na corporação, entende e analisa essas falhas de riscos, solucionando o problema e protegendo as informações e dados confidenciais de forma que seja aderida em todos os níveis gerenciais, com propostas que sejam atendidas inteiramente e confidencialmente para seu maior sucesso.

A forma de treinamento sobre segurança, tem que ser de forma mais ampliada, servindo prático na aprendizagem, mas não só restrito a isso, é necessário preparar pessoas para agirem em situações de riscos, identificando e neutralizando possíveis ações negativas.

Furtos, fraudes e espionagens na maioria dos casos ocorrem dentro das empresas com colaboradores descontentes, espiões, e desequilibrados sendo necessário a filtragem e retirada desses.

Por costumes e falta de adequação, na maioria dos casos os colaboradores apresentam resistências às normas internas e externas de segurança, porém é necessário ser avaliado que percebam os riscos que a inocência acarreta a grandes consequências.

Comprometimento a melhor forma de agente de prevenção aderindo a segurança.

Finalizando esse artigo, de forma ilustrativa, a Inteligência Estratégica e Segurança Corporativa Na Gestão de Pessoas" serve como primeiro filtro no processo seletivo, segundo filtro no colaborador em suas atividades e no processo demissional de agentes criminosos.

Fortalecer o elo entre colaboradores e corporação é uma missão vitoriosa.

Referências

CARVALHO, Luciana. **Casos de Espionagem Industrial.** Disponível em: <https://exame.abril.com.br/negocios>. Acesso em: 10 set.2018.

MITNICK, Kevin D.; Willian L. **O elo mais fraco é a segurança.** In: MITNICK, Kevin D.; Willian L. **A Arte de Enganar**. São Paulo: Pearson, 2003, p.21.

MITNICK, Kevin D.; Willian L. **Quando as informações não são inofensivas.** In: MITNICK, Kevin D.; Willian L. **A Arte de Enganar**. São Paulo: Pearson, 2003, p.45.

MITNICK, Kevin D.; Willian L. **Posso ajudar?** In: MITNICK, Kevin D.; Willian L. **A Arte de Enganar**. São Paulo: Pearson, 2003, p.22.

MITNICK, Kevin D.; Willian L. **Usando a simpatia, a culpa e a intimação**. In: MITNICK, Kevin D.; Willian L. **A Arte de Enganar**. São Paulo: Pearson, 2003, p.181.

MITNICK, Kevin D.; Willian L. **Usando a simpatia, a culpa e a intimação**. In: MITNICK, Kevin D.; Willian L. **A Arte de Enganar**. São Paulo: Pearson, 2003, p.197.

ROSSI, Lucas. **Sorria você está sendo vigiado**. Disponível em: <https://exame.abril.com.br/carreira>. Acesso em: 28 set.2018.

SLEIMAN, Cristina. **Ex funcionários acham normal levar dados corporativos após demissão**. Disponível em: <http://informationweek.itweb.com.br/12859/>. Acesso em: 12 out.2018.

EXAME. **Anonymous declara guerra cibernética à Rússia após invasão da Ucrânia**. <https://exame.com/tecnologia/anonymous-delara-guerra-cibernetica-a-russia-apos-invasao-da-ucrania/amp/>. Acesso em: 04 abr.2022.

BBC. **Anonymous: como hackers estão tentando minar Putin**. <https://www.bbc.com/portuguese/internacional-60813283>. Acesso em: 04 abr.2022.

BARRETO, Ricardo. **A evolução da inteligência competitiva**. <https://www.ricardobarreto.com/blog/index.php/2018/01/17/a-evoçuçao-da-inteligencia-competitiva/#:~:text=Passados%20mais%20mais%20de%202.000,da%20ci%c3%AAncia%20pol%c3%ADtica%20e%20criptografia%E2%80%A6>. Acesso em: 04 abr.2022.