O COMPORTAMENTO HUMANO: UM DESAFIO PARA A SEGURANCA CIBERNÉTICA

1° Ten Luiz Paulo Lopes dos Santos

Pós-graduado, lato sensu, em Guerra Cibernética

RESUMO: O Brasil passou por uma mudança de comportamento nas práticas diárias trazidas pela sociedade da informação, fazendo com que fossem aceitas alterações significativas nos valores sociais, profissionais e econômicos, sem a clara percepção de suas consequências a médio e longo prazo. Entre elas, destaca-se a necessidade de garantir a segurança cibernética por parte das infraestruturas de empresas e organizações. Será apresentado neste trabalho a preocupação que diversos países estão tendo acerca da segurança cibernética de suas estruturas. Ao longo deste trabalho veremos como a conduta humana pode prejudicar diretamente a segurança dos ativos de diversas organizações, bem como a falta de investimento de organizações e empresas para treinar e conscientizar seus funcionários para os riscos de ataques internos as suas estruturas. Concluímos que não adianta uma empresa ou organização somente investir em hardwares e softwares, se o elo mais fraco é o usuário, e que este pode simplesmente comprometer de forma irreversível uma rede. Por fim será sugerida alguma solução para minimizar as ameaças cibernéticas, como por exemplo, políticas de segurança cibernética dentro das organizações.

Palavras-Chave: segurança cibernética, comportamento humano, engenharia social.

1 INTRODUÇÃO

A parte da humanidade que tem acesso a algum nível de desenvolvimento econômico acostumou-se, em decorrência deste acesso, às facilidades em seu cotidiano para, de forma natural, realizar atividades que dependem de garantia de acesso às informações.

Com a internet, percebeu-se que muitas daquelas atividades podem agora ser realizadas mais rapidamente de forma eletrônica, por meio das Tecnologias da Informação e Comunicações (TIC). Como consequências do conforto oferecido pela internet, a humanidade passou a estar inserida na sociedade da informação, onde esta, o ativo mais importante, desempenha papel cada vez mais relevante na vida econômica, política e social das pessoas, organizações e nações.

Toda essa mudança natural de comportamento (aumento das interconexões das residências com os bancos, empresas públicas ou privadas e diversos níveis de governo) fez surgir o Espaço Cibernético, ambiente no qual está sendo construída uma verdadeira “nação virtual”.

Autorregulado e autônomo, o Espaço Cibernético permitiu a troca de informações das mais variadas formas, por pessoas e equipamentos, que fazem uso de toda essa infraestrutura crítica de informações, sem maiores conhecimentos técnicos de como esta troca se processa e sem uma clara percepção de suas consequências.

Essa falta de controle do Espaço Cibernético tem preocupado muitos Estados pelo fato de suas infraestruturas críticas estarem “conectadas” diretamente a este novo cenário virtual. Este artigo tem por finalidade elucidar organizações e empresas para uma ativo contra suas estruturas que é o fator humano.

Será também sugerido recomendações para minimizar vulnerabilidades nas infraestruturas críticas de uma organização, justificando o investimento em segurança cibernética dentro de organizações, incorporando o comportamento humano à análise, contribuindo para a formulação de políticas de segurança cibernética.

Desta forma, faz necessário analisar atitudes tomadas por essas empresas para buscar soluções para este problema, identificando comportamentos a serem considerados na análise de situações de falha de segurança cibernética, bem como quais as sugestões de condutas que busquem minimizar os riscos para que não ocorra a quebra de segurança cibernética.

2 O COMPORTAMENTO HUMANO

O comportamento humano é uma das principais fontes de vulnerabilidade na segurança cibernética de organizações. Inicialmente, deve- se partir do princípio de que não existe zero por cento de risco. Segue-se abaixo um trecho do artigo publicado por Roberta Prescott que aborda o fator humano como um dos pilares da segurança digital:

> "Por mais que todas as portas estejam protegidas (a última moda tem sido bloquear USB), que os processos sejam bem-estruturados e haja normas e código de ética, o elo mais fraco da segurança chama- se pessoas. [...] Ou seja, todo imenso investimento para proteger as informações cruciais pode ir por agua abaixo se a companhia descuidar do que elas têm de mais importante: os profissionais que ali trabalham". (PRESCOTT, 2007)

Segundo Kevin Mitinick:

> "Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam 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 configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis." (MITNICK; SIMON, 2003, p. 3)

Silva, M. Costa afirma que, um dos maiores problemas hoje em dia na segurança da informação está relacionado ao ser humano e à sua ignorância. A questão comportamental pode afetar significativamente as demais medidas de segurança, por mais modernas que elas sejam.

Essas práticas que permitem o acesso não autorizado aos dados, lugares, objetos e entre outros, fragiliza qualquer esquema de segurança da informação, uma vez que as pessoas acabam tendo acesso às informações indevidas, colocando em risco a segurança da instituição.

Apresentando análises de dados contidos no site do CERT.br (Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil), observa-se que no ano 2015, não considerando o Scan, o principal tipo de incidente reportado foi a fraude.

O Scan, segundo a legenda do CERT.br é a técnica de apenas verificar as redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles (é amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador) não causando um ataque efetivo ao sistema, como podemos ver na Tabela 1.

Essas fraudes, com o intuito de lesar ou ludibriar, podem, além de ser a enganação propriamente dita afim de se obter uma informação de alguém com cargo privilegiado, pode ser também a criação de páginas falsas, criadas para objetivos financeiros ou roubo de informações, bem como a 1ª invasão por programas computacionais (Cavalos de Troia).

A cibersegurança vem assumindo um papel importante dentro de organizações, mesmo que a maioria delas não priorizem as políticas de segurança e treinamento de seus funcionários, apenas em tecnologias de segurança e programas para seus sistemas informatizados.

Existe uma grande preocupação de organizações em garantir a segurança de seus sistemas informatizados, e mesmo com o au-

Tabela 1- Percentual de incidentes reportados pelo CERT.br referentes ao ano de 2015.

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2015

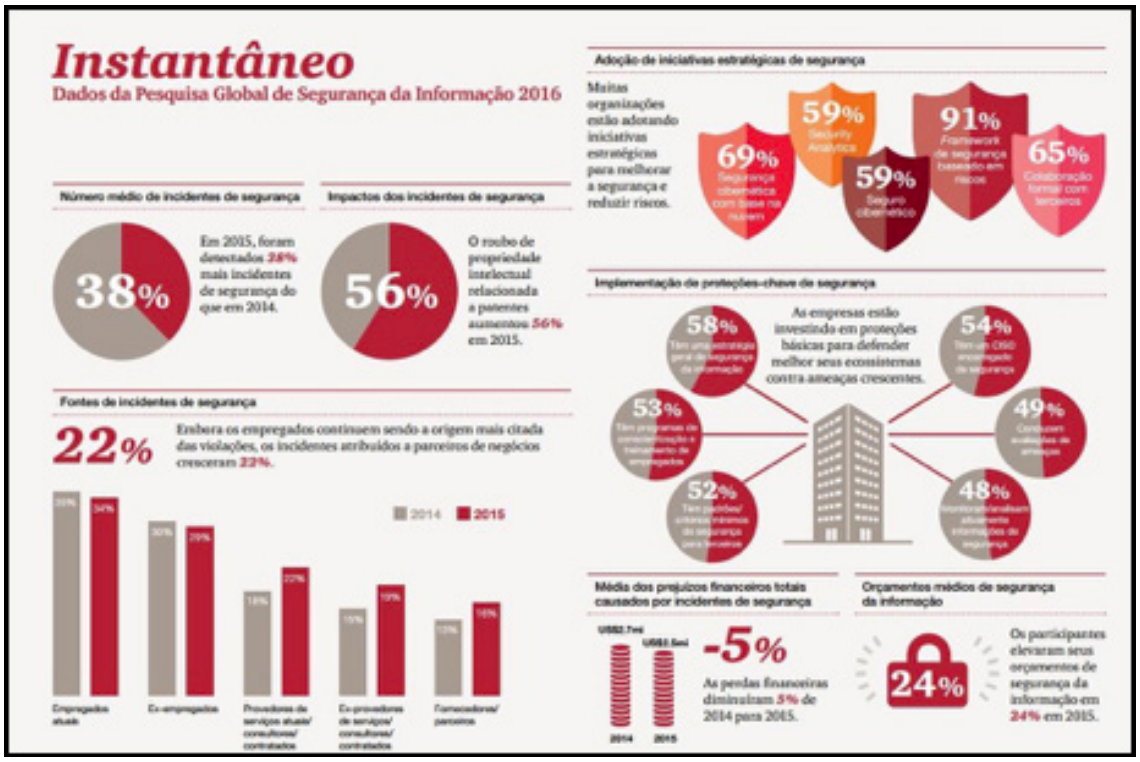
Tabela: Totais Mensais e Anual Classificados por Tipo de Ataque.

Mês	Total	worm (%)		dos (%)		invasão (%)		web (%)		scan (%)		fraude (%)		outros (%)	
jan	**67661**	2829	4	1367	2	409	0	6547	9	36445	53	18465	27	1599	2
fev	**66700**	2682	4	2056	3	289	0	8102	12	39267	58	12513	18	1791	2
mar	**52959**	2867	5	70	0	489	0	8822	16	32351	61	6338	11	2022	3
abr	**52991**	3046	5	34	0	150	0	6297	11	31215	58	10571	19	1678	3
mai	**58322**	3122	5	374	0	177	0	5399	9	23242	39	23890	40	2118	3
jun	**81244**	3423	4	1016	1	157	0	9219	11	29593	36	36327	44	1509	1
jul	**53075**	4141	7	2763	5	160	0	4716	8	32601	61	6561	12	2133	4
ago	**65486**	3683	5	3354	5	104	0	4447	6	33446	51	18701	28	1751	2
set	**59311**	4326	7	2511	4	119	0	3993	6	29759	50	16560	27	2043	3
out	**52226**	6301	12	1702	3	140	0	4315	8	32554	62	6089	11	1125	2
nov	**64203**	5912	9	9142	14	145	0	2297	3	38482	59	6595	10	1630	2
dez	**48027**	5390	11	971	2	118	0	1493	3	32268	67	6165	12	1622	3
Total	**722205**	47722	6	25360	3	2457	0	65647	9	391223	54	168775	23	21021	2

Fonte: http://www.cert.br

mento de 22% das violações e incidentes atribuídos a empregados, somente 53% das empresas têm programas de conscientização e treinamento desses agentes, mas não descartando as vulnerabilidades a infraestrutura da empresa que também tem de se melhorar com equipamentos de ponta, como podemos ver na FIGURA 1.

FIGURA 1- Percentual de incidentes reportados pelo CERT.br referentes ao ano de 2015.



Fonte: pwc, 2016.

A falta de preocupação das organizações em treinar seus funcionários é apresentada na tabela acima que em praticamente metade das empresas não ocorre essa preocupação.

Segundo Meirelles, em pesquisa da Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas:

> "Apesar das turbulências do cenário econômico brasileiro, com retração nas vendas, os gastos das empresas com tecnologia da informação se mantiveram estáveis em 2016/2017, ainda que em um nível bem inferior aos dos três últimos anos [...] os investimentos em TI permaneceram em 7,6% da receita das empresas nos últimos três anos. Segundo o levantamento, o setor de serviços, considerando as médias e grandes empresas, foi o que apresentou o maior aumento dos gastos com TI (11%), bem acima da indústria (4,5%) e do segmento de comércio, que se manteve como o que menos gasta e investe em tecnologia da informação (3,5%)" (MEIRELLES, 2017).

Pesquisa essa na qual podemos tirar conclusões, que as empresas investem em tecnologias, porém não em capacitação de recursos humanos para se prevenirem de ataques internos, vindo de seus empregados, ocasionados pela engenharia social.

O que se denominou recentemente engenharia social, há muitos anos já se chama ardil ou artifício fraudulento para o Direito Penal. Entende-se como engenharia social todo método de mascarar a realidade para explorar ou enganar a confiança de uma pessoa detentora de dados importantes a que se quer ter acesso.

Engenharia social, segundo Crespo (2011, p.82), é o artificio intelectual para acessar informações sigilosas e que, portanto, não utiliza necessariamente tecnologia, mas sim qualquer meio de comunicação.

Ataques desse tipo podem ter dois aspectos diferentes: o físico, como o local de trabalho, por telefone (call centers), no lixo (agendas telefônicas, organograma da empresa, manuais de sistemas utilizados), ou mesmo online.

Usando armadilhas e invenções intelectuais, um agente ativo de conduta delituosa acaba por persuadir um usuário inocente através da personificação.

Ataques de engenharia social tem como alvo as pessoas com um conhecimento tácito ou acesso às informações confidenciais, que muitas vezes assumem cargos de chefia, sem ter o discernimento da compartimentação de informação.

Segundo pesquisa realizada no dia 21 de setembro de 2011 pela empresa Check Pont Software Technologies, 48% das empresas pesquisadas foram vítimas de engenharia social, tendo 25 ou mais destes ataques no passado dois anos, custando às empresas valores entre U$ 25.000 a U$100.000 por incidente de segurança.

Outro dado interessante obtido pela empresa Check Point, é que há uma falta de formação proativa para prevenir ataques de engenharia social. Isso demonstra que 34% das empresas não tem qualquer treinamento de funcionários ou políticas de segurança no local para evitar essas técnicas, embora 19% tem planos para treinar seu pessoal contra-ataques de engenharia social.

3 CONCLUSÃO

A conscientização dos recursos humanos, acerca da segurança cibernética dentro de ambientes de trabalho, é importante haja vista de nada valer a melhor capacitação técnica se não conscientizar o usuário destas tecnologias, e de que a segurança cibernética é um problema de todos.

A grande preocupação de organizações é a priorização de seus investimentos em softwares de proteção e equipamentos, deixando de lado às políticas de segurança dos recursos de TI e treinamentos de seus funcionários.

Mesmo adquirindo programas computacionais de proteção, os índices de ataques tendem a aumentar, pois, definindo um padrão e boas práticas de segurança, o que não é um processo fácil, ainda assim não é possível determinar um padrão comum adequado para todas as organizações.

Estas organizações e empresas dão muita importância à segurança lógica de suas informações, porém não dada importância necessária aos seus usuários. Somente quando houver o equilíbrio entre a questão tecnológica e a questão comportamental humana que se alcançará níveis satisfatórios de segurança da informação organizacional.

Deve existir dentro das organizações um trabalho em relação à conscientização e treinamento constante dos usuários. A segurança cibernética pode ser encarada como um estudo multidisciplinar, no qual além de tratar das questões de segurança lógica e meios tecnológicos de segurança, também deve-se analisar o comportamento humano.

O profissional de segurança deve estar apto a se relacionar efetivamente com seres humanos com necessidades, atitudes e culturas diferentes, pois se o mesmo espera tratar apenas com computadores, não terá sucesso em alcançar os objetivos necessários para a segurança cibernética organizacional.

HUMAN BEHAVIOR: A CHALLENGE FOR CYBER SECURITY

ABSTRACT

Brazil underwent a change in behavior in the daily practices brought by the information society, making significant changes in social, professional and economic values accepted, without the clear perception of its consequences in medium and long terms. Among them, the need to guarantee cybernetic security by the infrastructures of companies and organizations stands out. This paper will present the concern that several countries are having about the cybersecurity of their structures. Throughout this work we will see how human conduct can directly harm the security of the assets of several organizations, as well as the lack of investment of organizations and companies to train and to make their employees aware of the risks of internal attacks on their structures. We conclude that it is no use for a company or organization to only invest in hardware and software, if the weakest link is the user, and that the user can simply irreversibly compromise a network. Finally, some solution will be suggested to minimize cyber threats, such as cyber security policies within organizations.

Keywords: Cyber security, human behavior, Social Engineering

REFERÊNCIAS

SILVA, Elaine M. da. Cuidado com a engenharia social, 2008. Disponível em: <https://www.tecmundo.com.br/msn-messenger/1078-cuidado-com-a- engenharia-social.htm> Acesso em: 19 mai. 2017.

MITNICK, Kevin D.; SIMON, William L. A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

PRESCOTT, Roberta. Fator humano: um dos pilares da segurança da informação. 2007. Disponível em: http://www.itforum365.com.br/seguranca/crimes-ciberneticos/fator-humano- um-dos-pilares-da-seguranca-da-informacao. Acesso em: 20 mai. 2017

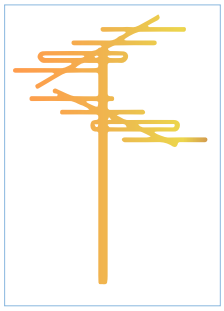
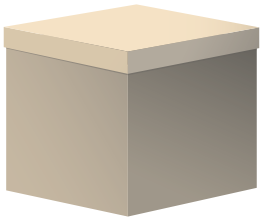
PWC, PricewaterhouseCoopers, Inovando e transformando em segurança cibernética, 2016. Disponível em: <https://www.pwc.com.br/pt/10minutes/assets/2016/pwc--10min-pesq-global- seg-inf-16.pdf> Acesso em: 20 mai. 2017

MEIRELLES, Fernando S. Tecnologia de Informação, 28ª Pesquisa Anual do Uso de TI, 2017. Disponível em: <http://eaesp.fgvsp.br/sites/eaesp.fgvsp.br/files/pesti2017gvciappt.pdf>. Acesso em: 23 maio 2017.

CHECK POINT SOFTWARE TECHNOLOGIES, Check Point Survey Reveals Nearly Half of Enterprises Are Victims of Social Engineering, 2011. Disponível em: <http://www.marketwired.com/press-release/check-point-

survey-reveals-nearly-half-enterprises-are-victims-social--engineering-nasdaq- chkp-1563778.htm> Acesso em: 25 maio 2017.

CRESPO, Marcelo Xavier de Freitas; Crimes Digitais. São Paulo: Saraiva, 2011.

License Type	FREE FOR COMMERCIAL USE WITH ATTRIBUTION LICENSE	
PREVIEW	DESCRIPTION	LICENSOR'S AUTHOR
	Antenna	Freepik
	Box	Freepik
	Box	Freepik

Icons made by Freepik from www.flaticon.com and br.freepik.com