SlackSpace

Teste de Penetração

Relatório EXECUTIVO

Cliente: ClienteXY

Uberlândia, março de 2018

SlackSpace Serviços LTDA – CNPJ 26.686.538/0001-95
Recuperação de Dados / Perícia Computacional / *PenTest*
34 3232-5111 / 34 99861-5111 – contato@slackspace.com.br
Rua República da Síria, 68 A - Uberlândia - MG

Sumário

1. Introdução

A SlackSpace Serviços LTDA executou, entre os dias 09/02/2018 e 27/02/2018 um teste de penetração do tipo cego, também chamado de *blackbox*, contra os ativos externos de tecnologia da empresa ClienteXY.

A prestação de serviços foi regida pela proposta comercial 011/2018 e contrato de prestação de serviços firmado em 07/02/2018.

Os resultados do trabalho executado são apresentados em dois relatórios:

- este relatório executivo, que apresenta em linguagem não técnica, uma visão geral: do ambiente, das vulnerabilidades, dos riscos e dos eventuais impactos de exploração das vulnerabilidades encontradas bem como recomendações para a solução dos problemas identificados.
- um relatório técnico, que apresenta todo o detalhamento técnico dos ativos identificados, suas informações detalhadas, as vulnerabilidades identificadas, os procedimentos executados e as recomendações técnicas para a solução dos problemas identificados.

Cumpre esclarecer que os testes foram feitos totalmente fora do ambiente do Cliente, nenhuma informação ou acesso privilegiado foi recebido ou utilizado. Todas as ações foram executadas da mesma forma que um atacante externo ao ambiente do Cliente poderia fazer. Com isso, obviamente, não foram testados servidores e ativos internos ao ambiente do Cliente; tal tipo de análise já configuraria testes do tipo *gray* ou *whitebox* que estão fora do escopo definido.

2. Escopo

2.1. Dentro do escopo

O serviço executado consistiu na execução de teste de penetração com o foco externo, do tipo *teste cego*, também chamado de *blackbox*; simulando um atacante existente em qualquer ponto da Internet sem informações detalhadas da empresa e sem acesso interno à rede do Cliente.

O escopo incluiu:

- servidor de hospedagem de páginas *web* e servidor de gerenciamento do site;
- servidor de correio eletrônico e acesso via *webmail*;
- servidor de hospedagem do domínio e de resolução de nomes;
- servidor de transferência de arquivos;
- site *web* do Cliente;
- *gateway* da rede interna do Cliente;
- serviços redirecionados a partir do *gateway*.

O escopo incluiu o levantamento de ativos, a busca de informações detalhadas dos ativos identificados, a identificação de vulnerabilidades e a definição dos riscos associados.

A tentativa de exploração das vulnerabilidades, ou seja: a invasão propriamente dita, foi feita apenas nos ativos do próprio Cliente; conforme descrito em proposta comercial previamente acertada.

2.2. Fora do escopo

Não fez parte do escopo da análise executada:

- rede interna do Cliente;
- rede sem fio do Cliente;
- nível de cultura em segurança da informação dos usuários do Cliente;
- testes e ataques de negação de serviço.

Parte do escopo estava hospedado fora do ambiente do Cliente, em provedores terceirizados. Para estes serviços, conforme proposta comercial, foram identificadas e testadas as vulnerabilidades, mas não foram feitas tentativas de explorá-las, pois tais ambientes são compartilhados e hospedam dados de vários outros Clientes o que implica em questões de ordem legal e prática.

3. Representação do ambiente analisado

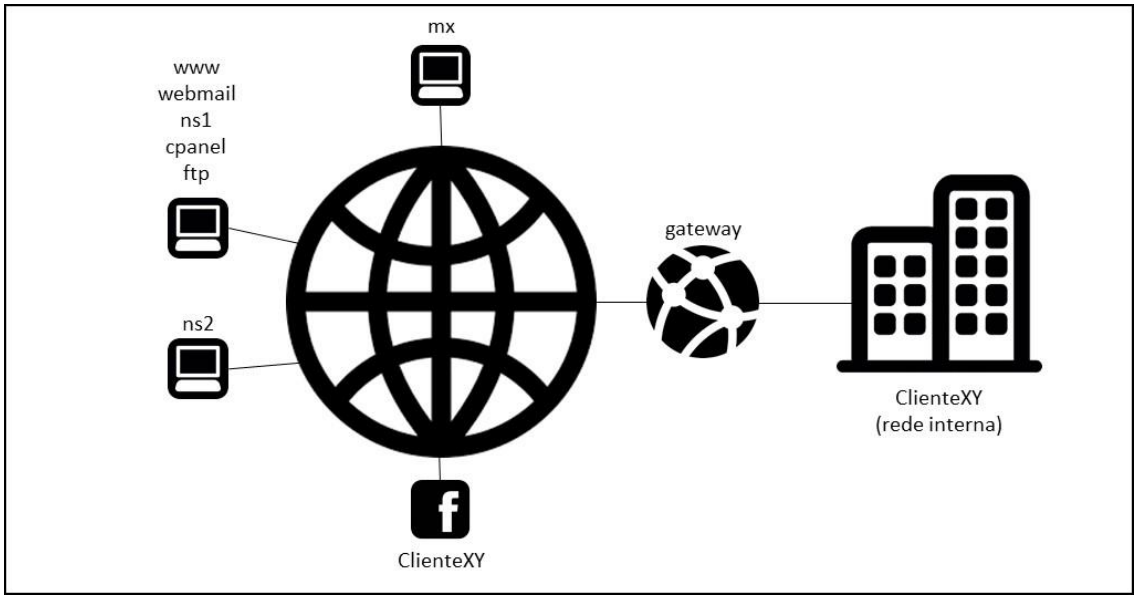

Figura 1 – Representação gráfica dos ativos mapeados

Foram mapeados 7 (sete) componentes de serviços. São eles:

- Servidor de e-mail
- Servidor de páginas
- Servidor de *webmail*
- Servidor de gerenciamento do site
- Servidor de transferência de arquivos
- Servidor de resolução de nomes primário
- Servidor de resolução de nomes secundário

Foi mapeado uma rede interna do cliente, com um *gateway* acessível via Internet.

Foi identificado um site institucional e um perfil na rede social Facebook.

4. Vulnerabilidades

Vulnerabilidades são falhas existentes em um *software* ou em um *hardware* e que são diretamente relacionadas à segurança do ativo ou de suas informações.

A partir da existência de uma vulnerabilidade, existindo também uma ameaça (alguém, algo ou algum *software*) em condições e disposta a explorar a referida vulnerabilidade passamos a contar com a existência de um Risco em potencial.

Se tal risco vier a se concretizar por meio da exploração da vulnerabilidade por uma ameaça, teremos um determinado Impacto no ativo, na informação ou no negócio do Cliente.

A Tabela 1 apresenta uma consolidação da quantidade de vulnerabilidades e suas criticidades por ativo. O detalhamento das vulnerabilidades é apresentado no Relatório Técnico.

		Vulnerabilidades			
#	**Ativo**	**Alta**	**Média**	**Baixa**	**Total**
01	Servidor 1	1	0	1	**2**
02	Servidor 2	1	4	1	**6**
03	Servidor 3	2	3	1	**6**
04	*Gateway*	1	1	1	**3**
05	Site *web*	0	1	4	**5**
	Total	**5**	**9**	**8**	**22**

Tabela 1 – Relação de vulnerabilidades por ativo com criticidade

5. Riscos existentes no ambiente

Um risco é uma possibilidade que algo ocorra, existem riscos bons e riscos ruins. Neste relatório tratamos dos riscos ruins, que podem afetar o negócio do Cliente; riscos relacionados à segurança de seus ativos, de suas informações, processos e em última instância riscos ao negócio do Cliente.

Para que um risco exista é preciso que existam: (1) uma vulnerabilidade que possa ser explorada; e (2) uma ameaça que possa explorar uma vulnerabilidade. Pela própria natureza da Internet e do mundo globalizado considera-se que a ameaça sempre existe; logo de forma simplificada a existência de uma vulnerabilidade (falha relacionada à segurança da informação) já implica em um determinado risco para o negócio do Cliente.

A partir da ciência da existência de um risco pode-se tomar a decisão de mitigá-lo por meio da: (1) correção ou do tratamento da vulnerabilidade que o originou; (2) da proteção contra a ameaça; ou (3) pode-se ainda decidir por assumir o risco e nada fazer para evitá-lo. Tal decisão pode ser baseada no eventual impacto causado ao negócio do Cliente.

O impacto que um risco pode causar no negócio do Cliente só pode ser determinado pelo próprio Cliente, pois é preciso conhecer o valor dos ativos, das informações armazenadas ou tratadas nestes ativos bem como os prejuízos advindos de eventual paralização do ativo; indisponibilidade das informações; divulgação indevida de informações...

De forma superficial, será apresentado impacto teórico juntamente com a apresentação dos riscos identificados.

#	Descrição do Risco (vulnerabilidade e ameaça)	Ativo	Impacto	Nível de risco teórico
01	Utilização do servidor para repasse de mensagens de terceiros com o consequente consumo de recursos computacionais bem como com a posterior inclusão em diversos serviços de lista negra de email/SPAM (item 4.2.1 #01)	Servidor 01	Serviços de e-mail lento para o recebimento ou entrega de mensagens e com bloqueio para diversos domínios	muito alto
02	Paralização: do site *web*, do gerenciamento do site *web*, da transferência de arquivos ou da capacidade de recebimento ou de envio de mensagens de e-mail por meio de negação de serviço na exploração de vulnerabilidade associada ao serviço MySQL (item 4.2.2 #01)	Servidor 02	Serviços paralisados comprometendo a operação do negócio	médio
03	Paralização: do serviço de resolução de nomes e transferência de zonas por meio de negação de serviço na exploração de vulnerabilidade associada ao serviço MySQL (item 4.2.3 #01)	Servidor 03	Serviços paralisados comprometendo a operação do negócio	médio
04	Exploração de falhas no site por meio das vulnerabilidades identificadas (item 4.3 #01 a #05) especialmente se futuramente forem agregadas mais funcionalidades de iteração no site além dos atuais formulários de contato	Site *web*	Furto ou uso indevido de informação	baixo

#	Descrição do Risco (vulnerabilidade e ameaça)	Ativo	Impacto	Nível de risco teórico
05	Visualização indevida de imagens geradas por câmeras de CFTV, inclusive de ambientes internos da empresa, por meio da descoberta de senhas fracas (item 4.4.2)	*Gateway*/ sistemas de CFTV	Prejuízo a imagem	muito alto
06	Alteração de configuração de sistemas de gerenciamento de CFTV com eventual paralização de gravação de imagens, trocas de senhas, ou outras configurações que impeçam o correto funcionamento do sistema por meio do acesso administrativo devido a adoção de senhas fracas (item 4.4.2)	*Gateway*/ sistemas de CFTV	Prejuízos a segurança física do ambiente do Cliente	muito alto
07	Prejuízo a imagem da empresa que fornece serviços de tecnologia em segurança por meio da divulgação indevida de imagens (item 4.4.2)	*Gateway*/ sistemas de CFTV	Prejuízo a imagem	muito alto
08	Prejuízo a imagem da empresa ou furto de clientes por meio da criação de perfis na rede social Facebook com identificadores já linkados no site institucional do ClienteXY, de modo que ao clicar no link disponível no site do ClienteXY, o Cliente seria direcionado a perfil no Facebook não gerenciado pelo Cliente (item 4.3.1.3).	Site *web* / rede social	Prejuízo a imagem	alto
09	Acesso indevido ao gateway do cliente por meio do serviço de telnet com o controle total do mesmo. O atacante poderia paralisar a conexão de Internet do Cliente ou poderia lançar mão de ataques mais sofisticados como envenenamento de DNS, mapeamento da rede interna, roteamento e acesso as máquinas da rede interna com a consequente exploração de vulnerabilidades na rede interna... (item 4.4.1 #01).	Rede interna e Internet	Prejuízo a imagem / Negação de serviços / Furto de informação	muito alto
10	Recebimento e execução de códigos maliciosos, incluindo vírus, vermes, malwares, ransomwares e outros em função da ineficiência ou ausência de sistema do tipo antivírus (item 4.5).	Rede interna e estações de trabalho	Prejuízo a imagem / Negação de serviços / Furto de informação	muito alto

Tabela 2 – Relação de riscos identificados

A Figura 2 apresenta uma representação dos riscos identificados em termos de criticidade baseados na exposição e impacto. Tais riscos foram identificados a partir das vulnerabilidades e ameaças existentes no ambiente. Não existe relação numérica entre as vulnerabilidades e riscos identificados pois algumas vulnerabilidades foram agrupadas num mesmo risco.

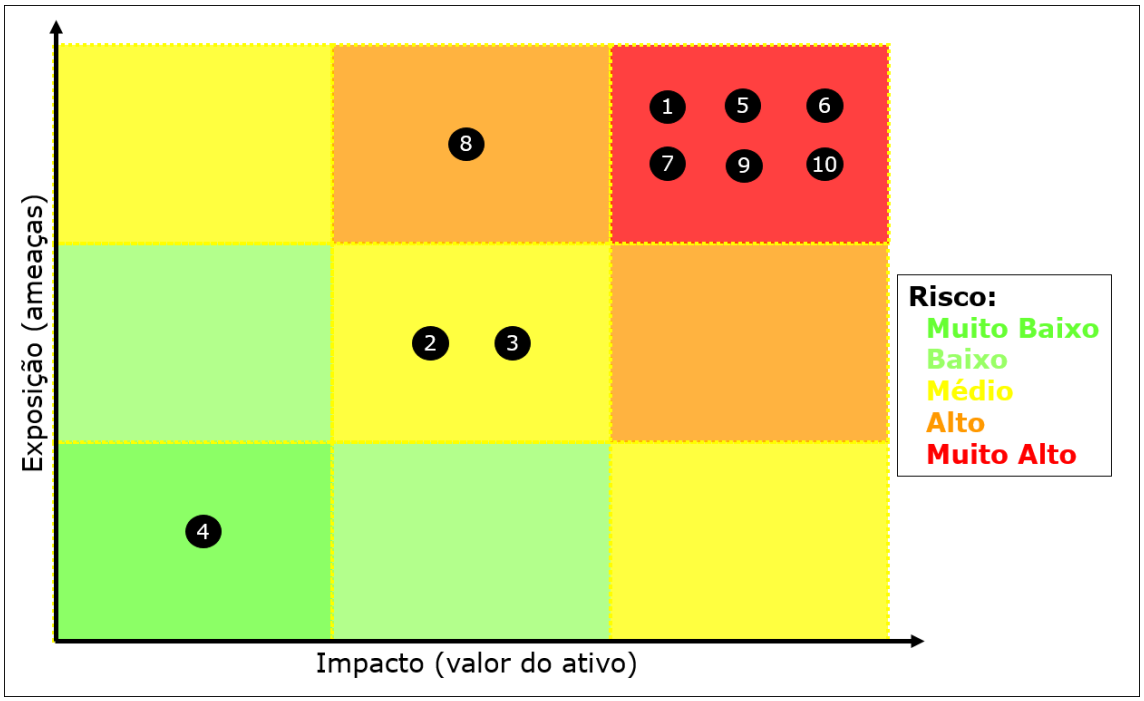

Figura 2 – Representação da criticidade dos riscos identificados

Cumpre informar que o ambiente conta com riscos considerados muito altos, alguns inclusive explorados durante o teste de penetração.

O *Pentester* obteve acesso completo e irrestrito ao sistemas de CFTV visualizando imagens internas inclusive; podendo apagá-las e alterar as configurações dos equipamentos. Também obteve acesso completo e irrestrito em uma estação de trabalho da rede interna, o que lhe permitiria a execução de dezenas de outros ataques a outras estações e eventuais servidores da rede interna. Tal acesso foi possível aproveitando-se da falta de cultura em segurança da informação do usuário bem como da ineficiência ou ausência de sistema antivírus. E de forma similar obteve acesso completo e irrestrito ao modem de acesso a Internet permitindo que vários outros ataques pudessem ser executados.

6. Recomendações gerais

No Relatório Técnico constam recomendações detalhadas para todas as vulnerabilidades identificadas, mesmo assim; faz-se necessário apresentar recomendações mais gerais que podem fornecer um caminho alternativo para a melhoria do nível de segurança do ambiente.

#	Recomendação	Abrangência
01	Substituir a provedor de serviços atual de *web*, e-mail e hospedagem de domínio por outro provedor com melhores práticas de segurança. O fornecedor atual mistura diversos serviços num mesmo servidor, inclusive serviços não utilizados pelo Cliente, o que eleva em muito a exposição do ativo e a propensão ao surgimento de novas vulnerabilidades.	Pode eliminar as vulnerabilidades apontadas para os servidores
02	Providenciar a correta configuração de modo a fechar o relay do servidor de e-mail	Elimina a possibilidade de uso indevido do servidor de e-mail
03	Providenciar a contratação de empresa de desenvolvimento *web* para a correção das vulnerabilidades e demais constatações quanto ao site *web* e redes sociais	Pode eliminar as fraquezas atuais do site e deixa-lo mais robusto para futuras novas funcionalidades
04	Providenciar a desativação do serviço de *telnet* no gateway para acesso via Internet	Elimina a possibilidade de acesso e reconfiguração do modem de acesso a internet bem como acessos indevidos a rede interna
05	Providenciar a substituição de todas as senhas dos sistemas de CFTV por senhas fortes e verificar as demais senhas utilizadas no ambiente do Cliente e em seus serviços externos	Pode eliminar os riscos associados a negação de serviço e a prejuízos de imagem advindos do acesso indevido aos sistemas de CFTV
06	Caso a recomendação 01 não seja adotada de pronto: desabilitar os serviços não essenciais (não utilizados) nos servidores 02 e 03	Pode melhorar o nível de segurança dos servidores
07	Caso a recomendação 01 não seja adotada de pronto: executar todas as recomendações técnicas emitidas na seção que apresenta as vulnerabilidades dos servidores	Pode melhorar o nível de segurança dos servidores
08	Refazer novo teste de penetração após substituição do provedor de serviços ou quando de mudanças significativas no ambiente de servidores ou do Cliente	Melhorar continuamente a segurança do ambiente
09	Testar a rede interna, rede sem fio, nível de cultura em segurança da informação dos usuários, bem como outros ativos não testados	Melhorar continuamente a segurança do ambiente
10	Verificar, atualizar e reconfigurar eventual sistema existente de antivírus ou implantar sistema de antivírus	Minimizar a possibilidade de execução de códigos maliciosos, e diminuir a probabilidade de ocorrência de perda de dados, divulgação indevida de dados, sequestro de dados e outros relacionados

Tabela 3 – Relação de recomendações identificadas

7. Conclusão

De forma geral, o nível de segurança do ambiente testado é regular. Porém conta com riscos altos que podem afetar severamente a imagem do Cliente.

A adoção das recomendações pontuais propostas pode elevar, em muito, o nível de segurança do ambiente.

É preciso deixar claro que a completa correção de todas as questões identificadas neste trabalho não implica em um ambiente totalmente seguro.

Isso se deve primeiramente pelo escopo contratado; pelo tipo de teste executado, que não inclui os ativos de rede interna bem como pela dinamicidade envolvida nos aspectos de segurança da informação e tecnologia.

No mais, é preciso ter a ciência que a segurança da informação deve ser tratada como um processo contínuo e deve ser constantemente verificada, testada e reforçada.

8. Sobre a SlackSpace

A SlackSpace preocupada com a ausência de empresas especializadas, nos segmentos de testes de penetração, recuperação de dados e pericia computacional na região de Uberlândia/MG, investiu em moderna estrutura, técnicas e equipamentos, bem como em profissionais extremamente capacitados; igualando-se as grandes empresas dos grandes centros no Brasil e no exterior.

A SlackSpace atua com total sigilo em três segmentos principais: na execução de testes de penetração; na recuperação de dados perdidos; e na elaboração de perícias computacionais.

Com sede própria, sua estrutura conta com ambiente que inclui laboratório de análise de vulnerabilidades e testes de penetração; laboratórios de recuperação de dados por problemas eletrônicos, físicos e lógicos; bem como modernos e completos laboratórios de perícia computacional.

Em seus quadros, conta com profissionais altamente especializados nestas áreas, profissionais com experiência prática de mais de 15 anos e com sólida formação acadêmica. A atualização constante dos profissionais e equipamentos é uma das mais importantes diretrizes de nossa empresa.