Os Perigos do Shadow IT

Ryan Karling[1]

[1] Instituto Federal Catarinense (IFC)

[2]Ciência da Computação - Segurança de Sistemas
Instituto Federal Catarinense (IFC) – Videira, SC – Brazil

karlingryan@gmail.com

Resumo. *Possivelmente você já soube de alguma empresa da região teve seus dados criptografados por um* ransomware*, está uma falha de segurança grave na organização que compromete todos seus ativos, expondo a riscos e vazamento de dados, a segurança de sistemas informatizados não se limita a antivírus e firewalls, ela vai muito mais além, o espaço físico e virtual podem ser ameaças do shadow IT, porém existem ferramentas e formas de reforçar a proteção dos seus ativos, diminuindo as ameaças e possíveis falhas.*

1. Os Perigos do Shadow IT

O *Shadow IT* é um risco no qual todos os ativos devem ser protegidos, inclusive o usuário, por possuir mais risco de facilitar o vazamento de dados, ou a entrada de agentes maliciosos em outros ativos. Em um ambiente corporativo, por exemplo, é necessário manter um controle rigoroso com acessos, permissões, políticas de firewall e utilização de dispositivos com I/O para usuário. Softwares sem licença ou de uso indevido, em ambiente controlado pode se tornar uma bomba no caso de uma auditoria ou perda de informações.

No IFC mesmo, por exemplo, se um aluno conectar um notebook, com algum malware na rede de um laboratório, e ela não possuir nenhuma proteção, todos os dispositivos serão infectados com um *Keylogger*, por exemplo. Os dados de todos que utilizarem estas máquinas estão comprometidos. Em contrapartida para evitar este tipo de ameaça existe o *CASB (Cloud access security broker)*, ele serve como uma camada de segurança, fazendo um proxy e um firewall extra na comunicação entre a rede e nuvem.

Através da visibilidade, analisa tudo o que é trafegado de um *workstation* até a nuvem, após este possui uma camada de integridade que garante que os dados trafegados não foram comprometidos por vírus e estão de acordo com a LGPD, fazendo um certo apoio a área de *compliance*. O CASB é um ótimo aliado no quesito segurança, capaz de identificar e criptografar dados sensíveis sendo trafegados na rede, controla o acesso a estes dados, também atua como um *proxy* unido ao firewall impedindo o usuário de acessar sites com pouca segurança ou executar softwares não licenciados.

Um detalhe muito importante é que em caráter de teste uma regra de firewall seja criada e esquecida pela equipe, ela pode se tornar uma vulnerabilidade. O CASB se encarrega de alertar sobre este risco. Podemos dizer que além de firewall, proxy, e antivírus ele é um *pentest*.

Dependendo da compatibilidade de softwares da sua organização e seu provedor em nuvem, o CASB pode atuar com coleta de logs, controle e análise de API's. Pode ser

um proxy forward e também pode realizar serviços de proxy reverso, sendo a borda de requisições, inibindo o contato da rede interna com a externa.

2. Mapeamento de Segurança

Ativos	**Ameaças**	**Requisitos de Segurança Afetados**
Dispositivos na rede da organização	Malwares, Worms, Ransmware, phishing, Vírus, Spywares, keyloggers	Privacidade
Usuários	Roubo e vazamento de dados.	integridade
Softwares da organização	Invasões físicas e virtuais	disponibilidade
Usuários	Falhas de segurança	não repúdio
Dispositivos Móveis de usuários	Usuários que usam softwares não autorizados	Confiabilidade
Softwares usados por usuários	Usuários sem conscientização de phishing e acesso a plataformas seguras	confidencialidade

3. Conclusão

Possivelmente você já soube de alguma empresa da região teve seus dados criptografados por um ransomware, está uma falha de segurança grave na organização que compromete todos seus ativos, expondo a riscos e vazamento de dados, a segurança de sistemas informatizados não se limita a antivírus e firewalls, ela vai muito mais além, o espaço físico e virtual podem ser ameaças do shadow IT, porém existem ferramentas e formas de reforçar a proteção dos seus ativos, diminuindo as ameaças e possíveis falhas.