NEWSLETTER

Segurança de Informação
e Continuidade de Negócio

MILLENNIUM BIM. AQUI CONSIGO.

Millennium bim

Edição de Dezembro de 2017

Ataques de Phishing

Estatisticamente, 95% dos ataques digitais se iniciam por *Phishing*, pelo que, é essencial abordar este tipo de ataque cibernético como forma de prevenção e protecção contra o mesmo.

O termo "*Phishing*" vem da combinação do termo em inglês "fishing", que significa pescar, com o termo "phreak", frequentemente usado para nomear os primeiros *hackers* de telefonia.

É um tipo de golpe que usa mecanismos tecnológicos, geralmente baseados em mensagens, para persuadir e enganar as pessoas, com um determinado objetivo, que varia de ataque para ataque. Actualmente, os ataques de *Phishing* aumentaram em complexidade e tamanho. .

Phishing

Phishing refere-se a um ataque que usa o *e-mail* ou um serviço de mensagens, como os de *sites* de media social, e que usa artimanhas ou induz para que se tome uma acção, como clicar num *link* ou abrir um anexo. A vítima de um ataque deste tipo corre o risco de ter suas informações altamente confidenciais roubadas e/ou o equipamento/dispositivo de trabalho ou pessoal infectado. Os criadores desse ataque envidam esforços por forma a tornar seus *e-mails* de *Phishing* convincentes. Por exemplo, eles elaboram o *e-mail* de tal forma que pareça que o mesmo tenha vindo de alguém ou de algo que lhe é familiar ou conhecido, como um amigo ou uma empresa confiável que utilize frequentemente. Adicionalmente, irão colocar logotipos do seu banco ou forjar o endereço de *e-mail* para a mensagem parecer mais legítima. De seguida, estes atacantes irão enviar esses *e-mails* de *Phishing* para milhões de pessoas. Eles não sabem de facto quem irá se tornar a vítima dessa acção, entretanto, quanto mais *e-mails* enviarem, maior será a chance de sucesso. *Phishing* é semelhante ao uso de uma rede de pesca, em que o pescador não sabe o que irá pescar, mas quanto maior for a rede, mais peixe irá provavelmente encontrar. Estes atacantes usam o *Phishing* de várias maneiras para almejarem os seus intentos, nomeadamente:

- **Colecta de Informações**:
  O objectivo do atacante é colher as suas informações pessoais tais como *passwords*, números de cartões de crédito ou dados bancários. Para o efeito, envia um *link* que o levará a aceder um *site* que pareça legítimo. Este *site*, em seguida, irá solicitar-lhe que forneça informações da sua conta ou os seus dados pessoais. Contudo, o *site* é falso, e toda e qualquer informação que a vítima digitar será visualizada pelo atacante.

- ***Links* Maliciosos**:
  O objectivo do atacante é tomar o controlo do seu dispositivo. Para fazer isso, eles enviam um *e-mail* com um *link*. Ao clicar no *link* o mesmo o navegará para um *site* que iniciará um ataque cibernéticono seu dispositivo que, se bem sucedido, infectará o sistema do mesmo;

- **Anexos Maliciosos**:
  O objectivo do atacante é o mesmo, infectar e assumir o controlo do seu dispositivo. Mas, ao invés de um *link* o atacante envia *e-mails* com um arquivo infectado, como um documento do Word/Excel/PowerPoint. Abrir o anexo desencadeiará o ataque, podendo dar ao atacante todo controlo do sistema do seu dispositivo;

- **Varreduras**:
  Alguns *e-mails* de *Phishing* não são nada mais do que os trapaceiros/burladores que se tornaram digitais. Eles tentam enganá-lo dizendo que ganhou na lotaria, fazendo-se passar por uma instituição de caridade que necessita de doações ou a pedir apoio para movimentar elevadas quantias de dinheiro. Ao menor sinal de resposta por parte da vítima a qualquer destas perguntas, eles irão solicitar um pagamento pelos seus serviços ou o acesso à sua conta bancária. O objectivo desses golpes é extorquir todo o dinheiro da vítima.

Proteja-se

Na maioria dos casos, abrir e ler um *e-mail* ou mensagem não constitui um problema. Para que um ataque de *Phishing* resulte os atacantes precisam induzi-lo a fazer algo. Contudo, normalmente, existem indícios de que uma mensagem é um ataque. E aqui estão os mais comuns:

- ✓ O *e-mail* cria um senso de urgência, exigindo "acções imediatas" antes que algo de mau aconteça, como por exemplo o encerramento da conta da vítima;

- ✓ Envio de um *e-mail* com um anexo que se desconhece ou um *e-mail* que solicite que a vítima abra o anexo. Os exemplos incluem um *e-mail* que informa que possui um anexo com detalhes de demissões não anunciadas, informação dos salários dos funcionários ou uma carta dos Órgãos Judiciais relativamente a um processo instaurado contra a vítima;

- ✓ Solicitações de *e-mail* sobre informação altamente sensível e confidencial, como o número de cartões de crédito ou *passwords*;

- ✓ O *e-mail* menciona que trata-se uma organização oficial, mas o conteúdo do texto exibe uma gramática ou ortografia medíocre, ou utiliza um endereço de *e-mail* pessoal, como @gmail.com ou @hotmail.com;

- ✓ O *link* parece estranho ou não oficial. Uma dica é passar o *mouse* sobre o *link* até que um *pop-up*/notificação mostre onde esse *link* o leva. Se o *link* no *e-mail* não corresponde ao destino do *pop-up*/notificação, convém que não se clique no mesmo. Em dispositivos móveis se pressionar o dedo num *link* recebe o mesmo *pop-up*/notificação. Um passo mais seguro é copiar e colar a URL do *e-mail* no navegador de *internet* do dispositivo ou digitar o *link* correcto;

Importa referir que os ataques de *Phishing* também tem ocorrido significativamente com a particularidade do seu envio ocorrer através de um SMS.

Estes SMSs são enviados tendo como remetente números móveis de vários dos operadores de redes móveis nacionais, através do mascaramento de números reais (fenómeno conhecido como *Caller ID spoofing*). Na maioria dos casos, os atacantes apresentam-se como estando ao serviço de entidades bancárias, mas também há registo de SMS ilegítimos, que são enviados em nome dos serviços postais ou marcas de retalho.

Caso acredite que esteja a ser vítima de um *e-mail*/mensagem/SMS que represente um ataque de *Phishing*, apague de imediato ou então informe a sua instituição bancária desse facto e comunique esse mesmo facto junto dos órgãos da polícia criminal ou das Autoridades Judiciárias. Em última instância, o bom senso é a melhor defesa.

Sabia que?

Eventos não previstos podem interromper as actividades e comprometer o desempenho, crescimento e até mesmo sobrevivência de uma organização. Pelo que, é de vital importância asseverar que as operações retomem o seu curso normal e previamente definido em caso de quaisquer incidentes. Assim, a **Continuidade de Negócio** é uma **ferramenta essencial** para assegurar que os objectivos definidos sejam atingidos mesmo quando a organização é exposta a algum **evento transitório ou disruptivo que possa interromper as suas operações de negócio.** O Grupo bim por estar ciente do exposto, possui uma política de Continuidade de Negócio que visa:

- **Instituir** níveis de prevenção e resiliência para mitigar o impacto de desastres.
- **Proteger** os Colaboradores, os activos e o negócio caso ocorra uma disrupção.
- **Apoiar** o breve retorno das actividades (críticas e normais) e, de todos os seus processos de suporte.
- **Consciencializar** os Colaboradores, os Clientes e as Entidades externas.
- **Garantir** que todos os procedimentos patentes no GCN são periodicamente testados e actualizados.

www.millenniumbim.co.mz