ESPIONAGEM
ECONÔMICA E INDUSTRIAL

PNPC
PROGRAMA NACIONAL
DE PROTEÇÃO DO
CONHECIMENTO SENSÍVEL

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Produção
Departamento de Contrainteligência
Programa Nacional de Proteção do Conhecimento Sensível (PNPC)

Projeto Gráfico
Coordenação-Geral de Relações Institucionais e Comunicação

Impressão
Divisão de Serviços Gráficos

ESPIONAGEM ECONÔMICA E INDUSTRIAL

2021

CONTEÚDO

PNPC | PROGRAMA NACIONAL DE PROTEÇÃO DO CONHECIMENTO SENSÍVEL

APRESENTAÇÃO

Esta cartilha tem o objetivo de apresentar a Espionagem Econômica e Industrial para gestores públicos e privados, empresários e profissionais de segurança da informação, a fim de prevenir ações de espionagem.

Este material foi elaborado pelo Programa Nacional de Proteção do Conhecimento Sensível (PNPC), desenvolvido pela Agência Brasileira de Inteligência (ABIN).

Criado em 1997, o PNPC é uma assessoria de segurança que busca promover cultura de proteção de conhecimentos sensíveis em instituições nacionais com foco na prevenção de ameaças como espionagem, sabotagem e vazamento de informações.

PNPC
PROTEGER COM INTELIGÊNCIA

1

O QUE É ESPIONAGEM?

Espionagem é a ação que visa à obtenção não autorizada de conhecimentos ou dados sensíveis para beneficiar Estados, grupos de países, organizações, facções, grupos de interesse, empresas ou indivíduos. São exemplos de ações de **espionagem:** pagar uma quantia em dinheiro a um funcionário do concorrente para furtar dados ou invadir o sistema de informações por meio de um ataque cibernético.

Tipos de espionagem

Espionagem de Estado

Ação que visa obter ou facilitar o acesso, indevido ou não-autorizado, a conhecimentos ou dados sigilosos, patrocinada direta ou indiretamente por um Estado nacional na defesa de seus **interesses estratégicos**.

Espionagem econômica

Ação que visa à obtenção de conhecimentos ou dados sigilosos cujo acesso indevido ou não-autorizado possa implicar a obtenção de **vantagens econômicas** para determinado Estado, ou para empresas consideradas vitais para a economia interna ou o desenvolvimento nacional desse Estado.

Espionagem industrial

Ação que visa ao acesso, indevido ou não-autorizado, de entidade não estatal a conhecimentos ou dados sigilosos de determinada instituição, empresa ou indústria que possam trazer o conhecimento de alguma **inovação técnica** que lhe garanta vantagens competitivas.

Espionagem comercial

Ação que visa ao acesso, indevido ou não-autorizado, de entidade não estatal a conhecimentos ou dados sigilosos de determinada instituição, empresa ou indústria que possam lhe trazer **vantagens comerciais**.

Estratégias de Estados Nacionais

É importante analisar se um Estado Nacional pode ser uma ameaça aos conhecimentos sensíveis da sua instituição, pois isso aumentaria seu risco de ser alvo de uma **ação mais elaborada** de espionagem.

Estados Nacionais têm a capacidade de **investir mais** na busca de informações, além de possuírem unidades especializadas para isso (os serviços de Inteligência) e outras estruturas que podem ser direcionadas para essa finalidade. Um Estado pode parar alguém na imigração de seu aeroporto e questioná-lo durante horas, por exemplo, ou interceptar comunicações que passam pela sua infraestrutura.

Uma empresa que pretende espionar um concorrente apenas realizará esse tipo de ação se puder obter **um lucro maior** em médio ou longo prazo do que o valor gasto com a espionagem, já que suas decisões são guiadas principalmente por uma lógica econômica. Um Estado Nacional, por sua vez, não necessariamente segue essa lógica de custo/benefício. Se o objetivo for considerado estratégico por um Estado, os recursos empregados na sua obtenção poderão ser maiores do que eventual lucro monetário.

Recentemente, entretanto, há casos de Estados Nacionais realizando ações seguindo uma lógica econômica, para conseguir recursos. Alguns países afetados por sanções internacionais, por exemplo, foram acusados de invadir sistemas de empresas privadas para criptografar todo o seu conteúdo, só liberando o seu acesso novamente após o pagamento de um “resgate”, o que é chamado de ***ramsonware***.

Você pode ser alvo de um Estado Nacional?

- Sua organização produz ou lida com informações de áreas estratégicas, como diplomacia, defesa ou pesquisa e inovação tecnológica?
- Sua organização tem concorrentes estatais?
- Sua área de atuação é estratégica para algum país?
- Sua atuação pode influir em alguma disputa entre outros dois países?

PNPC
PROTEGER COM INTELIGÊNCIA

2

GRADAÇÃO DE RISCO NAS AÇÕES DE ESPIONAGEM

Filmes de espionagem geralmente também são filmes de ação, em que o agente invade o local que abriga os conhecimentos sensíveis para furtar o que lhe interessa, saindo ileso apesar de todos os riscos envolvidos.

Na vida real, as ações de espionagem dificilmente envolvem ações ousadas como as dos filmes. Elas normalmente seguem uma **gradação de risco**, partindo das menos para as mais arriscadas. O agente da espionagem, independentemente de estar ligado a um Estado Nacional ou a uma empresa concorrente, buscará obter as informações com o menor risco e custo possível. Por que gastar dinheiro com algo que pode ser conseguido na internet ou em outras fontes abertas?

Ações de espionagem só são realizadas quando as informações obtidas por outros meios não são suficientes e o que se busca compensa o risco da operação.

Espionagem na vida real

Mesmo ações de espionagem costumam ser menos emocionantes do que as dos filmes. Em vez de invadir um local e furtar uma informação, um agente adverso, na maioria das vezes, irá agir sobre alguém que já tem **acesso legítimo** àquele conhecimento. Ao ser alvo de uma ação, essa pessoa poderá ceder essas informações sensíveis de forma involuntária, sendo enganada, ou mesmo de forma voluntária, desviando-as para o agente adverso.

No método mais comum encontrado no meio privado, uma empresa pode convencer um funcionário da empresa concorrente a **trocar de emprego**, levando consigo uma cópia das informações sensíveis em que tem interesse. Igualmente comum é que o próprio funcionário, mesmo não sendo instado pelo futuro empregador, copie as informações que utilizava no seu dia a dia e leve-as para auxiliar em sua nova instituição.

Outra forma de ataque é **simular negociações** apenas para obter as informações. Um grupo de supostos empresários pode pedir características técnicas sobre um produto, capacidades produtivas da empresa, custos e outras informações que seriam sensíveis e, depois, interromper os contatos. Mesmo países podem abrir negociações de compras internacionais apenas para obter informações que depois possam ser repassadas para suas estatais.

E se alguém simplesmente perguntar?

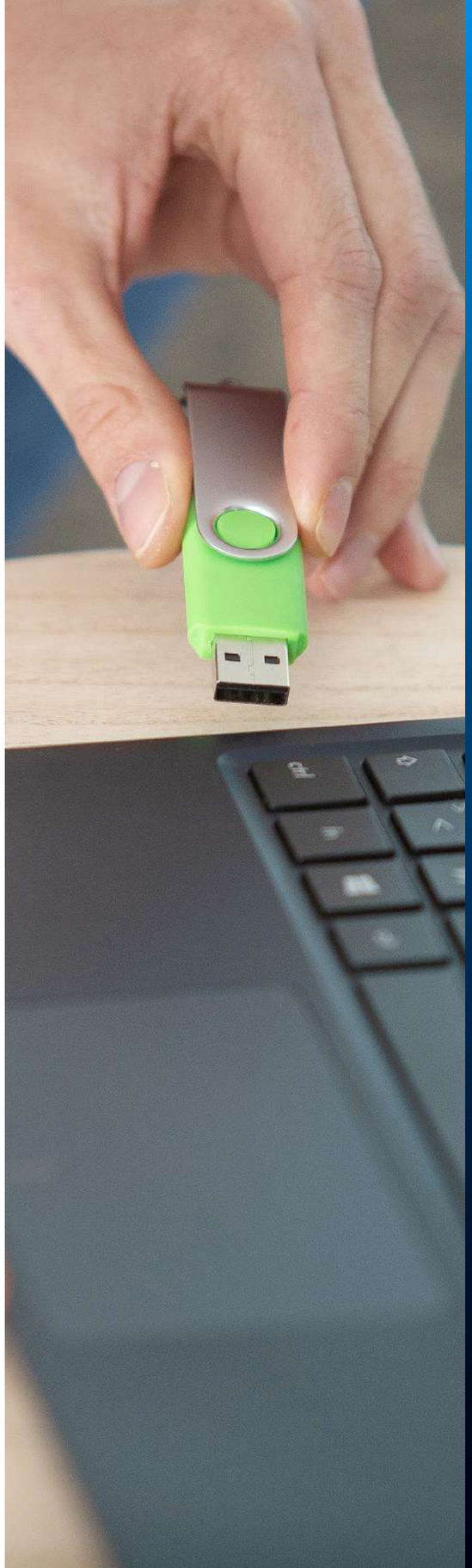
Pode parecer banal, mas uma técnica muito utilizada e com baixíssimo risco é **simplesmente perguntar** a informação sensível para a pessoa que a detém. Um funcionário pode receber uma ligação de alguém se apresentando como sendo de uma empresa de pesquisa e pedindo que o interlocutor responda a perguntas simples, entre elas, algumas sensíveis.

Nesse caso, o agente adverso ligará para diversas pessoas, bastando que uma responda para cumprir o seu objetivo. Por isso, ao perceber

que foi alvo de alguma ação, é importante que você reporte o caso para a equipe de segurança de sua instituição.

Outra forma de obter a informação é a chamada **entrevista**, em que o agente irá guiar uma conversa aparentemente casual com o alvo até obter a informação que deseja. Para a Atividade de Inteligência, a entrevista é uma conversa com propósito definido, planejada e controlada pelo entrevistador. Ela pode ser realizada para obter, confirmar ou fornecer dados ou ainda influenciar o comportamento de outra pessoa.

No intervalo de um congresso, por exemplo, o agente pode iniciar uma conversa. De um assunto, ele passará para outro, cada vez se aproximando mais de seu objetivo. A intenção é que o alvo passe a informação voluntariamente, sem nem ao menos perceber que o fez. O risco da técnica é relativamente baixo para o agente, que pode negar o ato.



Recrutamento

No mundo da espionagem, um agente adverso realiza ações especializadas para convencer uma pessoa a trabalhar, de forma consciente ou inconsciente, em benefício da Inteligência adversa. Ele recruta um alvo, por exemplo, quando o convence a fornecer, durante um **período extenso,** as informações sensíveis a que tem acesso devido à função que exerce em uma instituição.

Diferentemente de um funcionário que simplesmente copia informações antes de trocar de emprego, no recrutamento, o alvo permanece em sua instituição, explorando os acessos de que necessita para realizar seu trabalho.

As ações de **recrutamento** podem ser realizadas **diretamente,** quando o agente adverso sabe que o alvo tem alguma vulnerabilidade que pode ser utilizada de imediato. Alguém com um problema financeiro grave ou descontente com seu trabalho pode receber uma oferta direta de dinheiro em troca de informações.

A abordagem também pode ser **gradativa**. Nestes casos, o agente adverso normalmente inicia um relacionamento com o alvo para ganhar sua confiança. Depois, ele pedirá um primeiro favor, em geral, pequeno, que não gere um risco grande para o alvo e feito em nome da “amizade”. Após essa porta aberta, os pedidos vão aumentando de complexidade e pagamentos podem ser oferecidos. Nesse ponto, o alvo já está comprometido,

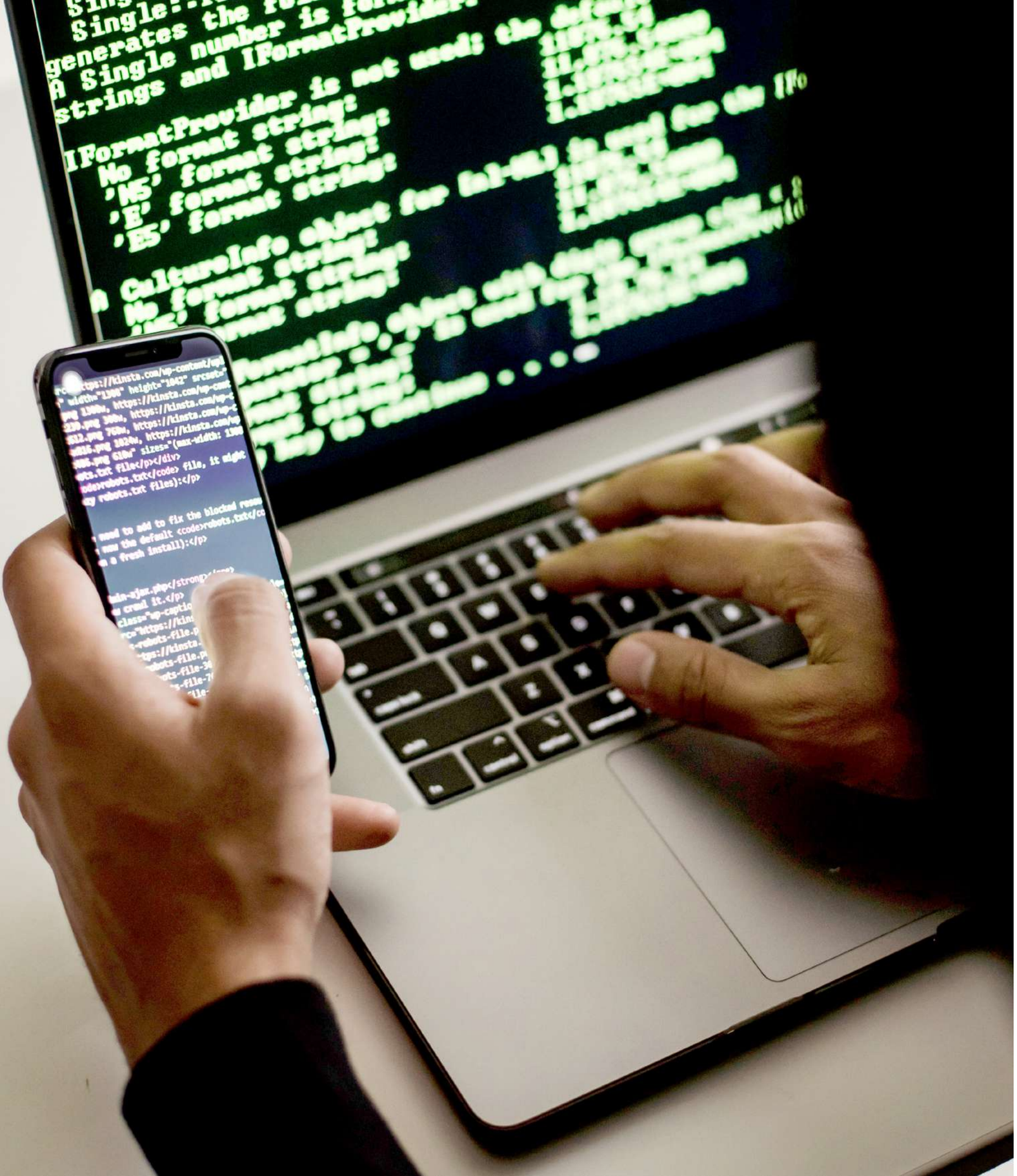
pois já forneceu informações que não poderia. Um arrependimento, agora, poderia gerar sua demissão ou sua prisão.

Quanto mais cedo o alvo notar a abordagem, mais facilmente conseguirá se livrar da ação. É importante que as instituições mantenham uma porta aberta para que funcionários nessa situação relatem o caso a fim de evitar um prejuízo ainda maior.

PNPC
PROTEGER COM INTELIGÊNCIA

3

ATAQUES CIBERNÉTICOS



Os casos de espionagem têm migrado cada vez mais para o ambiente cibernético, já que as informações de interesse costumam estar disponíveis nesse meio. Além disso, os ataques cibernéticos apresentam um **risco relativamente baixo** quando comparados às técnicas presenciais. Um agente pode atacar um alvo do outro lado do mundo sem se expor. Mesmo quando as ações são descobertas, atribuí-las a um ator específico é algo muito mais complicado do que no ambiente físico.

As imagens de filmes em que hackers invadem sistemas em minutos digitando alguns códigos em um computador também não refletem a realidade. Apesar de serem possíveis ataques puramente técnicos, ações cibernéticas costumam passar pelos usuários que detêm acesso legítimo aos sistemas de informação. Mesmo atores sofisticados, como serviços de Inteligência, utilizam a chamada **engenharia social** para conseguir invadir as redes de alvos.

Nesses casos, o agente adverso manipula uma situação de forma a convencer o alvo a realizar ação de seu interesse. Para inserir um malware em um sistema, por exemplo, ele pode enviar ao alvo um anexo de um e-mail contendo um documento contaminado. Isso funciona como uma porta que é aberta. Estando dentro do sistema, o agente pode utilizar outros meios técnicos para conseguir os acessos de que necessita até chegar às informações sensíveis.

Além de anexos de e-mail, outros meios podem ser utilizados para enviar arquivos contaminados, como redes sociais, aplicativos de comunicação (WhatsApp, por exemplo) e sites de download.

Além de arquivos, o agente pode tentar enviar links que direcionem o usuário a páginas falsas que peçam sua senha, depois utilizada para entrar nos sistemas reais. Sempre que receber um anexo ou um link, confira se realmente há necessidade de acessar aquela informação ou se é possível consegui-la de outra forma. Todo anexo e link trazem riscos para o sistema de informações.

Interceptação de comunicações

A espionagem vem inovando diante da miniaturização de dispositivos de interceptação de comunicações. Há relatos de Estados Nacionais que conseguem **implantar dispositivos** dentro de equipamentos eletrônicos antes mesmo que eles cheguem ao consumidor, permitindo a captação de todas as informações que trafeguem por ele. Essa implantação pode ser feita diretamente no fabricante ou interceptando uma carga durante o processo logístico.

Alguns países também conseguem captar todas as informações que **passam por sua infraestrutura de comunicações**. Como os dados não trafegam pelos caminhos mais curtos, mas pelos mais baratos, países com grande estrutura disponível concentram a maior parte do tráfego do mundo, conseguindo captá-los. Se sua instituição pode ser alvo de um Estado Nacional, os cuidados devem ser redobrados, com a adoção de meios criptográficos no fluxo de informações.

A **Internet das Coisas** tem facilitado o trabalho de interceptação de informações mesmo por agentes adversos menos sofisticados. Vários objetos cotidianos atualmente possuem conectividade à internet, mas apresentam requisitos de segurança menos rígidos. Problemas de configuração podem, por exemplo, deixar uma câmera de segurança acessível a qualquer pessoa pela internet. Um espião pode, potencialmente, se aproveitar de qualquer dispositivo com microfone (computador ou videogame, por exemplo) para ouvir uma conversa em outro país. Reflita sobre o ambiente em que assuntos sensíveis serão discutidos e avalie a necessidade de conectividade dos aparelhos presentes no local.

PNPC
PROTEGER COM INTELIGÊNCIA

4

PREVENÇÃO

Acesso mínimo

Como a maioria das ações de espionagem são realizadas sobre pessoas que possuem acesso legítimo às informações sensíveis, a melhor maneira de diminuir o risco é limitando esse **acesso ao mínimo** necessário para a realização das atividades diárias.

É comum, por exemplo, que setores não relacionados tenham acesso às informações uns dos outros, ou que um funcionário acumule acessos conforme mude de setor dentro da mesma empresa. Nesses casos, se apenas um funcionário for comprometido por um agente adverso, ele terá um volume grande de informações para passar.

Necessidade de conhecer

Por outro lado, caso os acessos às informações sejam limitados pela chamada **necessidade de conhecer**, esse funcionário passará uma quantidade menor de informações, diminuindo o impacto do evento.

Compartimentação

Identificados os grupos que necessitam de certos acessos, é possível limitar os fluxos de informações entre os grupos, o que é chamado de **compartimentação**.

Privilégio mínimo

Da mesma forma que as pessoas só devem acessar as informações de que necessitam para trabalhar, elas só devem conseguir rea-

lizar operações que realmente precisam no sistema de informações. Usuários normais não deveriam poder instalar softwares ou incluir e excluir usuários. Isso é chamado de **privilégio mínimo** e também ajuda a diminuir o impacto de um ataque cibernético.

Identificação

Quando um agente adverso realiza uma ação, seu objetivo é a informação. Qualquer pessoa que tenha acesso a ela é um possível alvo. Como normalmente vários funcionários podem chegar à mesma informação, os ataques costumam ser **campanhas**, atingindo várias pessoas da mesma organização em um curto espaço de tempo. Por isso é importante que os funcionários sejam capazes de **identificar** que estão sendo vítimas de uma ação adversa e que a **comuniquem** ao setor de segurança da instituição, para que ele consiga mitigar os danos.

Classificação

Nem todas as informações de uma empresa são sensíveis. Identificar quais merecem maior proteção evita impactos desnecessários nas operações cotidianas e gastos com medidas de segurança. As que forem identificadas, entretanto, devem ser **classificadas** como sensíveis e receber um tratamento especial.

Criptografia

A **Criptografia** é uma das principais ferramentas para proteção da confidencialidade de informações. Quando bem implementadas, soluções criptográficas reduzem muito o risco de espionagem. As principais vulnerabilidades, entretanto, estão nos usuários. Um arquivo pode ser transmitido encriptado, mas o usuário pode guardar uma cópia sem esse recurso em seu computador, facilitando o trabalho de um adversário. A senha utilizada também pode ser curta ou fácil de ser descoberta.

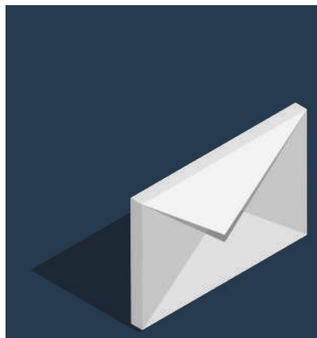
Aumento de Risco

Não existe sistema 100% seguro. Quanto mais recursos tiver o agente adverso, maior a probabilidade de obtenção de suas informações sensíveis. Deve-se buscar **aumentar o risco e o custo de uma ação adversa**. Se a porta de nossa casa permanecer aberta, um ladrão não terá nenhuma dificuldade de entrar. Se a porta estiver trancada, ele terá de utilizar alguma ferramenta para arrombá-la e levará mais tempo para conseguir entrar. Se tivermos um sistema de alarme, ele terá que ultrapassar esse obstáculo adicional, aumentando ainda mais o risco de sua ação.

Da mesma forma, na proteção das informações, quanto mais vulnerabilidades forem sanadas e quanto mais camadas de segurança forem adicionadas, mais recursos o adversário terá de gastar e mais riscos irá correr para conseguir chegar ao seu objetivo.

Treinamento

Como a maior parte dos ataques passa de uma forma ou de outra por pessoas que trabalham cotidianamente com as informações e sistemas de interesse para os agentes adversos, você não deve focar apenas em soluções tecnológicas. É fundamental conscientizar e treinar os **recursos humanos** em assuntos de segurança e incluir essa preocupação em todos os **processos** da sua instituição.



Reporte

Se perceber que foi alvo de uma ação direcionada a você ou à sua instituição, avise sua chefia e o setor de segurança. Você também pode enviar e-mail a **reporte@abin.gov.br** para estabelecer contato com a ABIN e relatar o caso.

PNPC

PROTEGER COM INTELIGÊNCIA

PNPC@ABIN.GOV.BR
WWW.GOV.BR/ABIN/PNPC