ManageEngine
Desktop Central

COMBATENDO **ATAQUES CIBERNÉTICOS** A **ENTIDADES GOVERNAMENTAIS**

VISÃO GERAL

O cenário de ameaças virtuais em 2020 parece sombrio. Noventa por cento das organizações acreditam que as ameaças virtuais piorarão no próximo ano, e 51 por cento ainda estão despreparadas para lidar com um ataque cibernético. As empresas não estão se planejando para todas as contingências possíveis, e qualquer organização pode estar na mira.

Algumas organizações, como as governamentais, são especialmente propensas a ataques; esse setor foi um dos principais alvos em 2020. A digitalização levou ao uso extensivo da Internet em todos os setores, aumentando a superfície de ataque em todas as empresas. É hora de reforçar a estratégia de segurança cibernética.

AS ENTIDADES GOVERNAMENTAIS SÃO **OS PRINCIPAIS ALVOS**

> Você sabia que **95% dos registros violados** em 2016 eram predominantemente de três setores: governo, varejo e tecnologia?

Esses setores não são menos diligentes do que outros em termos de segurança, então por que eles são muito mais atraentes para os hackers? Tudo se deve à grande quantidade de informações de identificação pessoal (PII) armazenadas em seus registros. Agências governamentais em todos os níveis, sejam federais, estaduais ou locais, possuem informações confidenciais que variam de datas de nascimento a números de CPF dos cidadãos. Em um nível micro, a perda desses dados pode facilitar o crime de falsidade ideológica mas, em um nível macro, segredos estatais podem ser expostos.

Não é surpresa que o governo dos Estados Unidos seja um alvo altamente visado. A Agência Nacional de Segurança (NSA) foi hackeada há alguns anos e, desde então, houve muitos ataques famosos de ransomware a cidades dos EUA. Aqui está uma breve recapitulação de alguns dos recentes ataques cibernéticos contra organizações governamentais dos EUA.

> Em dezembro de 2019, um ataque cibernético à **Nova Orleans** levou a cidade a decretar estado de emergência, desligando todos os computadores e servidores da cidade. No início de 2019, **o Texas sofreu um ataque de ransomware** que impactou os sistemas computacionais de 22 municípios, e os hackers exigiram o pagamento de 2,5 milhões de dólares para restaurar os arquivos. Em junho, a pequena cidade de **Lake City, na Flórida, sofreu um ataque de ransomware** que impediu que os funcionários do governo acessassem seus e-mails e fizessem transações on-line; a cidade acabou pagando um resgate de 460.000 dólares em Bitcoin. Outra cidade da Flórida, **Riviera Beach, pagou quase 600.000 dólares de resgate,** enquanto Nova Bedford, em Massachusetts, e Atlanta negaram-se a pagar os resgates exigidos pelos hackers e estão em processo de recuperar seus dados. A lista não termina aqui.

Seja o ataque à Rede de Informações da Segurança Interna em 2009, ou o ataque à cidade de Nova Orleans dez anos depois, os ataques cibernéticos continuam a assombrar as entidades governamentais e a pôr em perigo a economia global.

> **O relatório do Senado** revela que as agências governamentais reportaram 35.277 ataques cibernéticos apenas em 2017, uma média de quase 100 ataques por dia.

Como mencionado no relatório, dois grandes motivos pelos quais os governos são vítimas de ataques cibernéticos, além da falta de conhecimento especializado e orçamentos cada vez menores, são que eles não conseguem manter uma lista precisa de ativos de TI e não têm sistemas de patches automatizados para instalar patches de segurança.

As auditorias do Inspetor-Geral dos EUA também reconheceram que algumas agências governamentais utilizam sistemas herdados que não possuem mais suporte junto aos fornecedores, dificultando ainda mais a segurança desses sistemas. Talvez o fato mais surpreendente seja que o Departamento de Segurança Interna continue a usar sistemas desatualizados e não tenha conseguido solucionar brechas em seus sistemas.

COMO AS ORGANIZAÇÕES GOVERNAMENTAIS PODEM **COMBATER ATAQUES CIBERNÉTICOS?**

A base de qualquer organização são seus endpoints, sejam eles PCs, notebooks, smartphones, tablets ou servidores. As organizações governamentais devem tomar as seguintes medidas para proteger seus endpoints e combater ataques cibernéticos.

1 Avaliar e corrigir

É importante não perder o controle com cada vulnerabilidade que é identificada, pois uma vulnerabilidade nova é identificada a cada 90 minutos. Nem necessariamente todas as vulnerabilidades exigem atenção imediata. A magnitude das vulnerabilidades pode fazer com que pareça quase impossível avaliá-las, mas uma solução que consiga categorizar as vulnerabilidades descobertas e automatizar o processo tornaria a vida mais fácil para o departamento de TI. O mais importante para agências governamentais é ter uma solução capaz de avaliar e implantar os patches necessários automaticamente.

2 Seguir religiosamente o princípio de Zero Trust

Os funcionários do governo utilizam uma infinidade de dispositivos portáteis diariamente. Ameaças internas, incluindo a subtração de dados confidenciais usando dispositivos periféricos, como USBs, podem custar a uma organização até 8,76 milhões de dólares por ano. Embora seja verdade que 34% das violações de dados se devem a usuários internos, também é verdade que 70% das ameaças internas não são relatadas. O princípio da Zero Confiança pode revolucionar a estratégia de segurança cibernética de uma organização, protegendo contra ameaças internas.

Entidades governamentais podem evitar muitas ameaças virtuais se presumirem que nenhum indivíduo ou sistema pode ser automaticamente confiável. As organizações devem aplicar uma política de Zero Trust na qual todo dispositivo deve ser examinado quanto à sua adequação antes de ser autorizado. Além disso, os departamentos de TI devem monitorar os dados importados e exportados de dispositivos periféricos. Limitar transferências de arquivo com base no tamanho e no tipo de arquivo também pode ajudar a evitar a perda de dados.

3 Proteja os endpoints que a organização utiliza: os navegadores

Mais do que nunca, as organizações negligenciam os navegadores como fonte potencial de ataques cibernéticos; no entanto, eles são um dos meios mais fáceis de aplicar um ataque. Ataques virtuais a extensões, como a extensão para Chrome do Evernote Web Clipper, poderiam ser combatidos, em retrospecto, com uma solução que pudesse detectar as permissões possuídas por cada extensão e desativar automaticamente extensões que poderiam causar uma violação.

O phishing representa 90% das violações de dados. As organizações podem filtrar URLs e colocar sites confiáveis na lista de permissões para impedir que os usuários finais acessem sites mal-intencionados. Para proteger os dados, é altamente recomendável isolar os navegadores, pois, mesmo que um usuário final acesse um site mal-intencionado sem saber, a sessão da Web será aberta em um navegador virtual, evitando assim que malware infecte o sistema; os dados do navegador também serão apagados quando a sessão for encerrada.

4 Proteja todas as aplicações

Toda organização requer várias aplicações para operar de forma fluida. Custa caro para o departamento de TI manter o controle sobre as permissões concedidas a cada uma dessas aplicações. Para garantir que somente aplicações autenticadas acessem dados corporativos, é importante colocá-las na whitelist, desinstalar automaticamente as que estão na blacklist e impedir a instalação de aplicações de terceiros.

À luz das políticas BYOD (Bring Your Own Device, traga seu próprio dispositivo), as organizações governamentais devem implementar uma solução que consiga manter aplicações pessoais e corporativas em dois espaços virtuais separados. Em caso de perda ou roubo de dispositivos, as organizações precisam ter uma maneira de realizar uma limpeza completa dos dados e garantir que nenhum dado corporativo seja roubado.

5 Tenha uma visão panorâmica o tempo todo

Dashboards unificados podem fornecer às organizações governamentais uma visão rápida de todas as vias vulneráveis em potencial, para essas que possam impedir invasões em suas redes. As organizações devem monitorar auditorias de dispositivos, uso de navegadores, add-ons potencialmente perigosos, software desatualizado, máquinas altamente vulneráveis, o número de vulnerabilidades na rede e outras informações de segurança importantes.

As entidades governamentais devem avaliar o que está em jogo se um criminoso virtual se infiltrar em sua rede. As organizações devem fazer um inventário de todos os seus ativos de TI pelo menos a cada 24 horas para fazer com que a detecção de anomalias seja mais fácil. Também é recomendado nunca conceder acesso total a alguém que não precise. Ter uma visão centralizada de todas as permissões de usuário ajudará as organizações a monitorar os recursos que cada usuário pode acessar. Além disso, realizar backups frequentes e completos garantirá que os dados sejam guardados e protegidos e que o processo de recuperação, caso necessário, seja o mais simples possível. O ideal é que os backups ocorram com a frequência permitida pelos recursos.

CONCLUSÃO

Se tudo se resumir à questão de “devemos pagar o resgate ou não?”, apresentamos aqui alguns números preocupantes. Dos 39% dos profissionais de segurança que optaram por pagar o resgate após um ataque, menos de um quinto conseguiu recuperar seus dados críticos. Por exemplo, o caso NotPetya acabou sendo um caso de perda total para as vítimas que pagaram o resgate e não tinham seus arquivos descriptografados. Mesmo que uma organização consiga recuperar seus dados, ela ainda deve garantir que nenhum traço do ransomware seja deixado no sistema. Infelizmente, mais de 50% das empresas não têm orçamento para se recuperar de um ataque cibernético.

As organizações governamentais sempre enfrentaram uma batalha difícil contra os ataques cibernéticos. Embora o combate a eles seja uma tarefa árdua, com a ajuda de uma solução robusta de gerenciamento unificado de endpoints, o **ManageEngine Desktop Central,** as organizações governamentais estarão mais perto de interromper os ataques.

Entre em contato conosco para obter uma demonstração personalizada do Desktop Central. Você pode receber uma versão gratuita de teste por 30 dias para explorar nossa ferramenta.

Agende uma demonstração

Teste gratuito