RESTAURAÇÃO ABRANGENTE DE SERVIDOR COM A HEWLETT PACKARD ENTERPRISE

A HPE FORNECE CAPACIDADES DE RECUPERAÇÃO E SEGURANÇA LÍDERES NO SETOR EM SEU PORTFÓLIO PROLIANT GEN10

RESUMO

A proliferação de ciberataques amedronta todas as empresas e governos do mundo todo. Nações atacam a infraestrutura de TI de governos para desativar sistemas e paralisar os esforços de segurança nacional. Hackers sofisticados atacam entidades corporativas para roubar propriedade intelectual (PI), roubar dados de clientes ou sequestrar informações com o objetivo de pedir resgate.

A negação de serviço distribuída (DDoS) e outros vetores de ataque tradicionais estão rapidamente dando lugar a meios mais insidiosos. Mais de 91% dos ataques de ransomware vêm via anexos de e-mail.[1] Organizações de todos os tamanhos parecem reconhecer isso, já que mais de US$ 10 bilhões anuais serão gastos com o treinamento de segurança para funcionários.[2] No entanto, apesar de todo esse foco, os ataques de ransomware aumentaram 15 vezes em apenas dois anos e, no ano que vem, uma empresa será infectada com ransomware a cada 14 segundos.[3] Em termos mais amplos, o custo total da cibersegurança para a economia global chegará a US$ 6 trilhões até 2021 e US$ 8 trilhões até 2022.[4]

A pergunta não é "se" seu data center será atacado, mas "quando". Embora uma invasão na infraestrutura de TI possa ser inevitável, sofrer uma violação é completamente evitável. A pergunta que empresas de todos os tamanhos devem se fazer é: “Com que rapidez minha organização de TI pode detectar, isolar e remover malware; restaurar a infraestrutura para um estado reconhecidamente bom; e reinstalar sistemas operacionais, aplicativos e dados?” De acordo com um estudo da Accenture, o tempo médio entre o ataque por ransomware e a recuperação é de 23 dias. O custo médio? US$ 2,4 milhões. Quando uma grande transportadora foi recentemente vítima do ataque cibernético NotPetya, ela precisou restaurar mais de 4.000 servidores e 45.000 PCs em 10 dias.[5] Esse esforço incluiu limpar cada servidor e PC. Então foi preciso reinstalar sistemas operacionais e mais de 2.500 aplicativos, com todos os dados associados.[5] Embora a empresa não tenha atribuído publicamente um custo aos

esforços de recuperação, o dano total estimado foi de aproximadamente US$ 300 milhões.[6]

1-4: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
5: https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/
6: https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

A cibersegurança é um desafio multidimensional que requer uma resposta multidimensional. Moor Insights & Strategy acredita que as organizações de TI deveriam considerar uma segurança abrangente como requisito mínimo ao investir em infraestrutura de servidores. A segurança baseada no silício, complementada por ferramentas que permitem rápido tempo de recuperação, deve ser uma obrigação para qualquer servidor que seja instalado e conectado em qualquer data center. Ferramentas como a Server System Restore da Hewlett Packard Enterprise devem ser consideradas para gerar um rápido tempo até a recuperação. Na verdade, a MI&S não conhece nenhuma ferramenta de recuperação de servidor mais abrangente disponível no mercado.

ANATOMIA DE UM ATAQUE

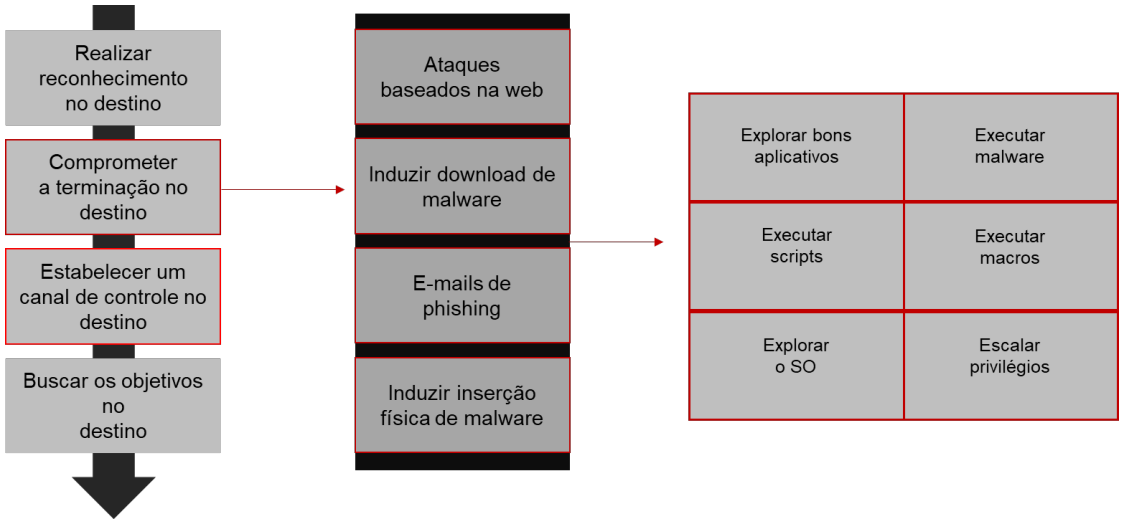
Os ciberataques contra data centers evoluíram consideravelmente. Os criminosos descobriram que não há necessidade de violar o perímetro enquanto houver um ser humano do outro lado de uma cadeia de e-mails. As maiores violações registradas são culpa de pessoas agindo como pessoas. Um pen drive deixado no chão de um estacionamento em um prédio de uma base militar dos EUA no Afeganistão levou ao maior comprometimento de computadores militares dos EUA na história, e foram necessários 14 meses para recuperar.[7] Uma senha escrita à mão e deixada à vista de todos resultou na infame violação do Target em 2013.[8] E as senhas armazenadas sem segurança no GitHub levaram à violação do Uber em 2016.[9]

O processo de atacar uma organização pode ser dividido em quatro fases distintas:

- *Reconhecimento* – Identifique o alvo. Procure por fraquezas óbvias para explorar. Planeje o ataque (DDoS, e-mail de phishing, etc).
- *Violação* – Envie o e-mail de phishing. Insira o malware via USB ou outros meios. Execute o ataque DDoS.
- *Conquista de um canal/plano de controle* – Insira o malware no ambiente por diversos meios.
- *Execução do plano* – Baixe. Criptografe. Apague. Distorça.

7-9: Afirmações de James Morrison, um Cientista Computacional do FBI, junho de 2017

FIGURA 1: AS FASES DE UM CIBERATAQUE



Fonte: Moor Insights & Strategy

Se estiver achando tudo muito militarizado, é porque é assim mesmo. Ataques contra entidades governamentais e corporativas são tudo, menos aleatórios. As nações são as criadoras de muitas das ferramentas de hackers existentes. E, na verdade, essas nações são frequentemente as perpetradoras. Considere também a quantidade de dinheiro em jogo. Como mencionado anteriormente, os ciberataques custarão à economia global aproximadamente US$ 6 trilhões em 2021, que é um terço do GDP dos EUA e mais que todo o comércio de drogas ilegais do mundo.

Bootkit e *firmware* são provavelmente os ataques mais danosos. Esses ataques permitem que os criminosos obtenham acesso a um servidor abaixo da camada do sistema operacional. Esse nível de acesso permite ao malware permanecer presente, embora virtualmente indetectável até mesmo a tecnologias modernas de segurança implantadas no data center. Os ataques de Firmware também são os mais difíceis de combater, e os mais prováveis de permanecerem não detectados − com uma média de 99 dias antes de serem descobertos.

Por mais difícil que seja manter o controle sobre firmware de servidor na corporação, as organizações de TI não estão bem preparadas. Em um estudo feito pela Information Systems Audit and Control Association (ISACA), apenas 8% das empresas tinham medidas adequadas estabelecidas para controlar e gerenciar o firmware em seus ambientes.

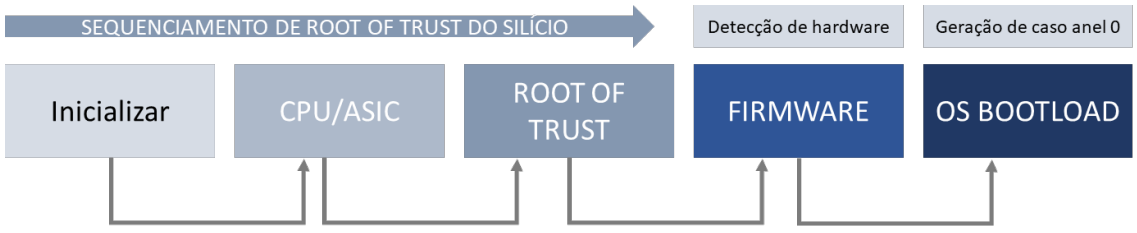
PROTEÇÃO CONTRA ATAQUES

Embora não exista uma “bala de prata” para proteger o seu data center, o MI&S encontrou algumas plataformas de servidor que empregam mecanismos de segurança que oferecem altos níveis de proteção. Uma delas é o portfólio de servidores Gen10 ProLiant da Hewlett Packard Enterprise.

A Root of Trust de silício da HPE fornece proteção assim que o servidor é ligado e o firmware Integrated Lights Out (iLO) entra em ação. À medida que o servidor é inicializado, seu firmware é comparado com uma impressão digital imutável armazenada no iLO 5 para verificar se todo o código do firmware é válido e não comprometido.

Se algum malware ou código comprometido tiver sido inserido na ROM do sistema UEFI do firmware iLO 5, o silício irá detectá-lo porque o código de firmware infectado seria alterado e, dessa forma, não ocorreria uma equivalência (com o hash gravado no silício). O UEFI, então, valida a conexão com o sistema operacional por meio de inicialização segura, concluindo assim uma raiz ou cadeia completa, que é ancorada no silício. Outro firmware essencial do servidor também é validado, para incluir o CPLD, M.E., I.E. e Option ROM, completando, assim, a verificação de quase 4 milhões de linhas de código de firmware.

FIGURA 2: ROOT OF TRUST DE SILÍCIO DA HEWLETT PACKARD ENTERPRISE



Fonte: Moor Insights & Strategy

Simplificando, a Root of Trust de silício da HPE cria uma impressão digital imutável que é usada para validar o firmware. As alterações no firmware são identificadas rapidamente, permitindo que as organizações de TI respondam mais rapidamente aos ataques de firmware.

RECUPERAÇÃO DE ATAQUES

Objetivo de tempo de recuperação (RTO), tempo de recuperação de trabalho (WRT), tempo de inatividade tolerável máximo (MTD) são termos com os quais a maioria dos profissionais de TI está familiarizada. Esses termos ajudam a definir a tolerância de uma organização por tempo de inatividade em cenários de recuperação de desastre. A maior parte dos planos de recuperação de desastres (DR) foram criados antes da ameaça real de ciberataques e, como resultado, estão incompletos. Recuperações de ciberataques são tradicionalmente confusas. Em essência, os servidores devem ser recriados do firmware até os sistemas operacionais, para aplicativos e dados. Em um ambiente corporativo, essa tarefa pode parecer impossível, mesmo com as ferramentas de gerenciamento de configuração disponíveis na maioria dos fornecedores de servidores. Essas ferramentas tendem a não ter a integração e as confirmações seguras para garantir uma recuperação completa e oportuna que não reintroduza o malware em um ambiente do qual ele foi removido.

A Moor Insights & Strategy acredita que há três coisas que as organizações de TI devem exigir das ferramentas de recuperação empregadas.

- ***Segurança -*** Vasculhar 5.000 servidores de malware apenas para reintroduzir esse malware ao reinstalar um sistema operacional é um problema real vivenciado pelas organizações de TI corporativas. Uma “confirmação” segura da recuperação de firmware para o repositório que contém imagens ISO, aplicativos e dados é uma necessidade absoluta.
- ***Capacidade de expansão -*** Busque ferramentas de recuperação que possam restaurar o data center em escala. A transportadora levou 10 dias para restaurar 4.000 servidores, o que é impressionante, mas o tempo de inatividade custa aproximadamente US$ 200 milhões. A capacidade de restaurar esses 4.000 servidores em paralelo reduziria muito o impacto financeiro.
- ***Simplicidade –*** Como a função entre a TI e os negócios continua a se confundir, as ferramentas usadas na restauração de servidores devem fornecer recursos de restauração quase que de clique único. Uma ferramenta abrangente difícil de usar é uma ferramenta abrangente que não terá uso.

As organizações de TI idealmente deveriam implantar uma plataforma de segurança cibernética altamente integrada. Ou, no mínimo, deveriam implantar ferramentas que compartilhem o DNA. Ou seja, as ferramentas usadas para proteger um ambiente residem no mesmo portfólio de tecnologia das ferramentas usadas para se recuperar

de ataques cibernéticos. Isso garante os mais altos níveis de integração e deve levar à solução mais completa.

RESTAURAÇÃO DO SISTEMA PARA SERVIDORES HPE

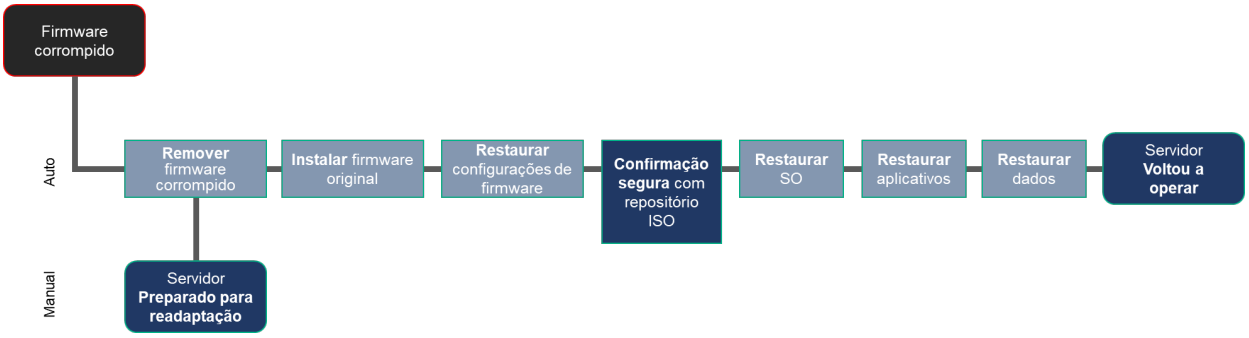
A Restauração do sistema para servidores é um recurso do iLO Amplifier Pack da Hewlett Packard Enterprise. Ele fornece com segurança a restauração automática de até 10.000 servidores com um único clique.[10] O que torna esse recurso excepcionalmente poderoso é sua capacidade de gerenciar incidentes cibernéticos de forma tão completa para servidores HPE Gen10 que possuem o iLO Advanced Premium Security Edition instalado. Quando um servidor é detectado com firmware corrompido, os administradores de TI podem ativar uma das três respostas:

- ***Restauração automática***:
  - Firmware corrompido é removido.
  - O firmware essencial de servidor não comprometido verificado é reinstalado

10: Testes internos da HPE – fevereiro de 2017.

  - As configurações de firmware são recuperadas e instaladas, economizando tempo para recriar manualmente as configurações.
  - A confirmação segura é estabelecida com o repositório ISO, que impede a instalação de imagens corrompidas.
  - A facilitação de uma restauração do SO a partir de um ISO está concluída.
  - A restauração facilitada de aplicativos foi realizada.
  - Recuperação dos dados de um repositório de backup secundário protegido.
  - Servidor volta à operação.
- ***Restauração manual:***
  - Firmware corrompido é removido
  - O firmware de servidor não comprometido verificado é reinstalado.
  - O servidor de destino é deixado em um estado limpo, aguardando a ação do profissional de TI (por exemplo, redirecionar o servidor)

FIGURA 3: OPÇÕES DE RESTAURAÇÃO DO SISTEMA PARA SERVIDORES



Fonte: Moor Insights & Strategy

No momento deste relatório, a Hewlett Packard Enterprise parece ter a oferta de segurança mais abrangente de um grande fabricante de servidores em sua linha Gen 10. A segurança baseada em Root of Trust de silício pode reduzir drasticamente o tempo necessário para detectar ataques de firmware. E a Restauração do sistema para servidores oferece o que a Moor Insights & Strategy enxerga como fatores críticos em um processo de restauração; segurança, escalabilidade e simplicidade. Essas soluções formam o que pode ser a cadeia de confiança mais segura no setor de servidores.

CHAMADA À AÇÃO

O mundo está mudando. Implantar aplicativos Web de três camadas com uma DMZ e firewall não é mais suficiente para proteger o datacenter. A aquisição e o uso de malware para atacar organizações é mais simples e mais frequente do que nunca. E as organizações afetadas parecem mais dispostas do que nunca a pagar o resgate a um criminoso em troca da devolução dos dados do cliente.

A Moor Insights & Strategy enxerga as organizações de TI de pequeno a médio porte como o principal alvo rico dos hackers. Isso se deve à quantidade de dados armazenados combinados com medidas de segurança menos abrangentes. Porém, seja gerenciando um data center, uma sala de servidores ou um gabinete - seus dados estão em risco.

À medida que as empresas gastam dezenas de bilhões de dólares em software de segurança ou implantam redes definidas por software para gerenciamento baseado em políticas, os níveis mais baixos de hardware ficam vulneráveis a ataques de root kit que podem causar estragos por meses antes da detecção.

A Moor Insights & Strategy acredita que empresas de todos os portes devem procurar acelerar os projetos de modernização da infraestrutura para aproveitar melhor os recursos de segurança que podem oferecer proteção desde o silício. Essas novas plataformas de servidor também fornecem os recursos para as capacidades de recuperação mais abrangentes em resposta a um ataque cibernético.

A Hewlett Packard Enterprise é a única grande fornecedora de servidores que fornece a Root of Trust de silício e uma recuperação abrangente por meio da Restauração do sistema para servidores. Por isso, organizações de todos os portes devem considerar a implantação do HPE iLO 5 Amplifier Pack e do iLO Advanced Premium Security Edition.

INFORMAÇÕES IMPORTANTES SOBRE ESTE DOCUMENTO

COLABORADOR
Matt Kimball, analista sênior da Moor Insights & Strategy

EDITOR
Patrick Moorhead, fundador, presidente e analista-chefe da Moor Insights & Strategy

DÚVIDAS
Fale conosco se quiser discutir este relatório; a Moor Insights & Strategy responderá prontamente.

CITAÇÕES
Este documento pode ser citado por membros da imprensa ou analistas credenciados, mas deve ser citado em contexto, exibindo o nome do autor, o cargo do autor e "Moor Insights & Strategy". Pessoas que não sejam da imprensa nem analistas devem receber autorização prévia por escrito da Moor Insights & Strategy para qualquer citação.

LICENCIAMENTO

DECLARAÇÕES DE ISENÇÃO
Este documento técnico foi encomendado pela Hewlett Packard Enterprise (HPE). A Moor Insights & Strategy fornece pesquisa, análise e consultoria para muitas empresas de alta tecnologia mencionadas neste documento. Nenhum funcionário da empresa detém qualquer posição como acionista de qualquer empresa citada neste documento.

ISENÇÃO DE RESPONSABILIDADE
As informações apresentadas neste documento têm propósito informativo somente e podem conter imprecisões técnicas, omissões e erros tipográficos. A Moor Insights & Strategy nega qualquer garantia de precisão, integralidade ou adequação de tais informações e não deve ser responsabilizada por erros, omissões ou inadequações de tais informações. Este documento contém somente opiniões da Moor Insights & Strategy e não deve ser interpretado como afirmações de fatos. As opiniões expressas neste documento estão sujeitas a alterações sem aviso.

A Moor Insights & Strategy fornece prognósticos e declarações prospectivas como indicadores direcionais, não como previsões precisas de eventos futuros. Embora nossos prognósticos e declarações prospectivas representem nosso discernimento atual sobre o que o futuro reserva, eles estão sujeitos a riscos e incertezas que podem fazer os resultados reais diferirem em termos materiais. Advertimos para não depositar confiança indevida nesses prognósticos e declarações prospectivas, que somente refletem nossas opiniões no momento da publicação deste documento. Por favor, tenha em mente que não nos comprometemos a revisar ou divulgar publicamente os resultados de qualquer revisão desses prognósticos e declarações prospectivas de acordo com novas informações ou eventos futuros.