PAESSLER
THE NETWORK MONITORING COMPANY

WHITE PAPER

Sua Segurança é Segura?

White Paper

PRTG NETWORK MONITOR

Author: Thomas Timmermann, Senior Manager Technical Marketing, Paessler AG
Publicado em: Abril 2016

Conteúdo

Introdução 2

As maiores ameaças da TI 3

Tarefas da Solução de Monitoramento 3

Lista de Checagem de Avaliação 4

- Recursos de monitoramento abrangentes mais API 4
- „All Inclusive“ 4
- “Comportamento Incomum” 4
- Armazenamento de Dados 4
- Publicação de Dados 4
- Usabilidade 5
- Preço e Licenciamento 5
- Teste 5

Introdução

Muitas tendências quentes em TI acabam se revelando – depois de um curto período de tempo – como meros fogos de artifício de véspera de Ano Novo: Um grande estrondo, que brevemente se acende e, por fim, se apaga. Mas este não foi o caso da Segurança, também chamada simplesmente de Security. Desde os primeiros dias da rede, a Security foi um dos principais problemas da TI, agora mais do que nunca. Isso foi comprovado em uma pesquisa realizada pela Paessler AG em 2015, na qual 58% dos administradores entrevistados indicaram que uma de suas principais tarefas e desafio constante é a segurança de TI. Enquanto anos atrás um firewall e um antivírus ainda eram suficientes para proteger a rede de PMEs e seus respectivos dados de circulação, hoje se entrelaça uma série de soluções diferentes para neutralizar as ameaças em constante evolução. Todas estas ferramentas de segurança podem garantir uma segurança abrangente, mas apenas se sua função é protegida e se a visão geral é assegurada em todas as medidas. Isto requer uma estratégia de segurança abrangente que identifica riscos potenciais, introduz ferramentas adequadas como uma proteção preventiva e deixa tudo ser controlado e mapeado por uma solução central.

As maiores ameaças da TI

Vírus e cavalos de Tróia não são menos perigosos, só porque eles existem desde os primeiros dias da Internet. Volta e meia, novos malwares aparecem nas manchetes de jornal e, devido à expansão da rede, mais e mais portas são constantemente abertas para toda e qualquer coisa. Por isso, o uso de scanners de vírus, firewalls e sistemas de detecção de intrusão ainda se justifica.

Traga seu Próprio Dispositivo (BYOD) ou a Internet das Coisas (IoT) cria novas oportunidades para incidência de malware. Onde uma vez bastava uma simples proibição de discos, CDs ou USB drives privados, hoje muitos dispositivos se conectam com a rede. A proibição geral não é praticável e tão pouco sensata em muitas empresas: Muitos funcionários usam smartphones, tablets ou laptops particularmente e profissionalmente e, assim, aumentam a sua eficiência. Até mesmo a IoT cria novas portas de entrada, integrando muitos dispositivos na rede que não pertencem à TI atual e, por isso, seu potencial de risco é muitas vezes difícil de avaliar. O departamento de TI deve conhecer com antecedência tais riscos e encontrar o compromisso certo entre as novas possibilidades e maior flexibilidade, por um lado e a segurança necessária por outro lado.

Não só os invasores mal-intencionados ameaçam os seus dados: Falhas ou dispositivos e aplicativos mal configurados também podem causar perda de dados. Não se trata de construir muros de proteção, mas sim um sistema de monitoramento e de alerta, que possa constantemente monitorar todos os componentes críticos e, em caso de falhas, imediatamente possa reagir ou, na melhor das hipóteses, já possa ver os primeiros sinais de problemas iminentes e avisar antes que a situação se torne crítica.

Não apenas os riscos sistêmicos ameaçam a TI, também desastres físicos como incêndios, inundações, calor ou roubo não podem ser desconsiderados em um conceito de segurança abrangente. Para que serve o melhor software antivírus, quando o centro de dados está sob a água ou o ar condicionado na sala do servidor falha e a temperatura atinge níveis críticos.

Para praticamente todas as ameaças, há o “antídoto” ideal. Scanners de vírus e firewalls protegem contra malware, ferramentas de backup asseguram os dados, sensores monitoram a umidade e temperatura ambiente enquanto câmeras de vigilância mantêm intrusos indesejados sempre a vista. Enquanto todos estes sistemas estiverem confiáveis, sua TI é relativamente segura. Mas como você se certifica de que tudo funciona? E acima de tudo: Como você mantém o controle do número de sistemas que são essenciais para a segurança da sua TI? Para um conceito abrangente de segurança, você precisa de uma solução de monitoramento que aja como uma espécie de ferramenta de meta-segurança para o controle e gestão das medidas individuais.

Tarefas da Solução de Monitoramento

As definições de vírus estão atualizadas? Todos os backups válidos foram criados? O firewall está online? Somente se as ferramentas de segurança trabalharem com confiança, a segurança é garantida. A solução de meta-segurança deve ser capaz de monitorar ferramentas tradicionais de segurança e garantir o seu funcionamento correto. Mas o que acontece quando um vírus não é detectado ou um cavalo de Tróia é ignorado pelo firewall? Neste caso, a solução de monitoramento deverá detectar o respectivo comportamento incomum, como um aumento elevado de tráfego, enchimento rápido da memória ou tráfegos de e-mail atípicos e, imediatamente, avisar sobre o grau de perigo.

Soluções de monitorização adequadas monitoram continuamente o desempenho e a função de todos os componentes de sua infraestrutura de TI, independentemente quando se trata de hardware, software ou fluxo de dados. Assim você evitará perda de dados e garantirá condições de trabalho ideais para os seus colegas. Além disso, a solução de monitoramento deve ser capaz de monitorizar a função de sensores físicos, tais como câmaras de vídeo e assim assegurar que todos os sistemas estejam trabalhando bem como manter perigos imanentes de TI e riscos físicos em vista e, se necessário, notificar ou alertar em caso de irregularidades.

Manter tudo a vista é um aspecto central de um conceito da segurança abrangente. Somente se você sempre for capaz de visualizar rapidamente e facilmente todas as suas ferramentas de segurança, sem ter que solicitar cada solução individualmente, só assim você terá uma chance de manter o controle contínuo da situação geral de segurança. A solução de monitoramento deve ser capaz de integrar todas as ferramentas utilizadas e reproduzi-las facilmente em uma única exibição.

Nem toda ferramenta de monitoramento é capaz de cumprir todas estas tarefas. Algumas não proporcionam as funções necessárias, outras são muito caras, outras muito complexas e caras. Abaixo uma visão geral dos critérios que devem ser considerados durante uma avaliação.

Lista de Checagem de Avaliação

RECURSOS DE MONITORAMENTO ABRANGENTES MAIS API

É muito importante que a solução em questão traga consigo todas as funções para monitorar toda a infraestrutura de TI e dominar muitos dos protocolos padrões, tais como SNMP, Ping, FTP, HTTP, NetFlow, sFlow, jFlow, WMI ou Packet Sniffing. Porém, nenhuma solução de monitoramento pode monitorar toda a sua TI logo de cara, pois infra-estruturas modernas são altamente complexas e heterogêneas. Assim, em conjunto com uma API bem documentada, quase todos os dispositivos e aplicativos podem ser vigiados – também outras ferramentas de segurança, sensores, câmeras de vigilância, etc. E quando tudo isso ainda forfácil de implementar com o uso de modelos e exemplos, então você praticamente já encontrou a solução adequada.

"ALL INCLUSIVE"

Muitos sistemas de monitoramento são oferecidos como um kit composto e exigem para quase qualquer função um add-on pago. Isso muitas vezes gera custos significativos. Certifique-se de que seu candidato de monitoramento ofereça muitas opções já na versão básica e lhe informe sobre módulos posteriores já no seu cálculo inicial.

"COMPORTAMENTO INCOMUM"

Claro, você precisa definir limites personalizados para alertas e alarmes em sua solução de monitoramento. Além disso, o software também deve ser inteligente o suficiente para reconhecer um comportamento incomum, mesmo que os limites definidos não sejam atingidos. Por exemplo, se um vírus começa a produzir um aumento do tráfego na rede, uma solução inteligente pode detectar o aumento atípico e informá-lo sobre isso imediatamente para que você possa tomar medidas oportunas.

ARMAZENAMENTO DE DADOS

A maioria das soluções de monitoramento usa bancos de dados SQL para armazenar os dados de monitoramento. Bancos de dados SQL não são projetados para armazenar dados de monitoramento (registros muitos pequenos que entram cronologicamente em intervalos curtos, e para os quais nenhum acesso de escrita é necessário), por isso estes dados geralmente não podem ser armazenados no formato RAW, ao invés disso eles são compactados como valores médios. Isto pode ser problemático, especialmente quando uma solução de monitoramento é usada como uma ferramenta de segurança, se uma pesquisa de longo prazo seja necessária para identificar as vulnerabilidades.

PUBLICAÇÃO DE DADOS

Dados de monitoramento são publicados de maneiras diferentes:

- Como uma exibição ao vivo na forma de painéis ou mapas sobre diferentes superfícies. Certifique-se de que a solução não traz apenas uma interface gráfica do Windows, mas pelo menos ainda uma interface web e, se possível, aplicações para sistemas móveis populares. Os painéis e mapas devem ser ajustáveis de forma individual e permitir a representação de dados em uma forma clara e atraente: Gráficos bonitos e bem processados são uma festa para os olhos e geram prazer e, portanto, são percebidos com mais atenção do que tabelas e listas antiquadas e feias.
- Como relatórios, geralmente em formato HTML ou PDF. Estes relatórios podem ser feitos com ferramentas padrão ou ferramentas de terceiros, on-the-fly ou regularmente em horários especificados. Relatórios geralmente oferecem a opção de exibir os dados de um período definido. Isto torna possível mapear e interpretar dados históricos.

Idealmente, a solução deve fornecer relatórios, bem como maneiras de criar facilmente painéis e mapas personalizados. Aqui a opção muito interessante é gerar mapas HTML personalizados, nos quais todos os elementos do conceito de segurança podem ser claramente exibidos. Também é possível até mesmo posicionar a planta de um edifício como imagem de fundo, na qual há sensores físicos, câmaras de vigilância, e similares.

USABILIDADE

Mesmo se uma nova solução de monitoramento for introduzida e instalada como ferramenta de meta-segurança em um projeto: Se a solução for muito complexa para o uso diário, provavelmente ela não será usada suficientemente. Um software de segurança não utilizado não é apenas um investimento inútil, ele também constitui um risco de segurança. Pois nestes casos, a presença da solução dá uma imagem de segurança que, na verdade, não existe. Portanto, a facilidade de uso do software deve estar no topo da lista na hora da avaliação. Às vezes, até faz sentido dispensar um ou outro recurso adicional, se a aceitação e a facilidade de uso da solução forem garantidas.

PREÇO E LICENCIAMENTO

Preço e tipo de licença também têm um papel importante na compra de uma solução de monitoramento. Importante aqui é, em especial, a transparência. Todas as tarifas estão disponíveis? O processo de licenciamento é compreensível? Se os módulos e add-ons estão disponíveis, quais você precisará desde o início ou no futuro previsível? Muitas vezes há armadilhas de custos escondidas na forma de módulos ou você terá de fazer um upgrade de licenciamentos depois de um curto período de tempo devido a modelos de contrato difíceis de entender.

TESTE

Instalar e testar o software! Não confie em listas de recursos, consultores ou até mesmo no marketing do fabricante. Uma solução meta-segurança é um elemento chave em um conceito de segurança abrangente. Somente se o software “se sentir bem” ele encontrará a aceitação necessária para ser capaz de cumprir o seu papel. Mas se já a versão de teste for difícil de obter ou complicada para instalar, então há o perigo de que a versão completa venha com sérios problemas.

SOBRE A PAESSLER AG

O premiado PRTG Network Monitor da Paessler é uma poderosa solução de Monitoramento Unificado, de custo acessível e de fácil utilização. Ele é extremamente flexível, uma solução universal para monitoramento de Infraestrutura de TI, atualmente utilizado por organizações e empresas de todos os tamanhos e segmentos. Mais de 150.000 administradores de TI de mais de 170 países contam com o PRTG para terem tranquilidade, confiança e comodidade. Fundada em 1997 e baseada em Nuremberg na Alemanha, a Paessler AG opera até hoje como empresa privada e é parceira dos programas Cisco Solution Partner Program e VMware Technology Alliance Partner.

Aprenda mais sobre a Paessler e o PRTG em www.paessler.com.br

Paessler AG
www.paessler.com.br, info@paessler.com