ESTUDO DE CASO

Fortinet garante alto nível de disponibilidade e desempenho de rede durante os Jogos Olímpicos da Juventude

Ao lado dos Jogos Olímpicos e as Olimpíadas de Inverno, os Jogos Olímpicos da Juventude são um dos maiores eventos esportivos internacionais do mundo. Em cada edição, o Comitê Olímpico Internacional (COI) trabalha com a cidade-sede para coordenar a organização deste evento que reúne, presencialmente e virtualmente, milhões de espectadores do mundo inteiro. A última edição dos Jogos Olímpicos da Juventude foi em Buenos Aires, Argentina, em outubro de 2018. Este evento de 12 dias reuniu 4.012 jovens atletas, representando 206 delegações de diferentes países. Esta última edição também alcançou um número recorde de espectadores: 1,1 milhão de pessoas compareceram aos 16 locais de competições das diferentes modalidades esportivas.

Em eventos deste porte e magnitude, a segurança física dos atletas sempre é uma prioridade. Porém, nos dias de hoje em que as informações e os dados são armazenados e transportados pela rede, a segurança dos dispositivos e a disponibilidade da infraestrutura de TI também provaram ser aspectos fundamentais para os organizadores do evento. A equipe de segurança de TI da prefeitura de Buenos Aires foi encarregada de gerenciar todos os aspectos de cibersegurança do evento, incluindo uma avaliação de riscos preliminar para um evento internacional dessa natureza, a definição de processos para resolvê-los e a adoção de firewalls da próxima geração da Fortinet, que oferecem segurança avançada, para ajudar a garantir a disponibilidade da rede e prevenir e mitigar incidentes.

Proteção da infraestrutura de TI de um evento internacional de grande escala

O processo começou três anos antes do início das competições, logo depois que Buenos Aires foi anunciada sede dos Jogos Olímpicos da Juventude de 2018. A equipe de segurança de TI da prefeitura desenvolveu um plano para implementar a infraestrutura de TI, os sistemas e a solução de cibersegurança dos jogos de Buenos Aires.

"Precisávamos encontrar uma solução completa que garantisse disponibilidade, acessibilidade e desempenho da rede sem comprometer a segurança durante os Jogos Olímpicos da Juventude. É por isso que decidimos adotar o pacote FortiGate da Fortinet completo, com todos os seus recursos, incluindo controle de IPS, filtro web, proteção avançada contra ameaças e todos os serviços associados, em cada local e nos datacenters centrais. O fato de termos um parceiro tecnológico capacitado nos permitiu detectar incidentes que já havíamos mapeado, encontrar uma solução e implementá-la rapidamente para mitigar riscos potenciais de cibersegurança, tudo isso sem diminuir a disponibilidade ou o desempenho da rede."

– *Gustavo Linares, diretor-gerente de segurança de TI da prefeitura de Buenos Aires.*

"Conversamos com outras entidades para definir a implementação de redes específicas para os Jogos Olímpicos em cada um dos 16 locais de competição. Para a segurança dos dispositivos, montamos três linhas de trabalho: uma voltada para a prevenção, uma para a operação, e outra para a resolução de incidentes e análise forense", explicou Gustavo Linares, diretor administrativo de segurança de TI da prefeitura de Buenos Aires.

Os requisitos e solicitações mais importantes do comitê organizador estavam relacionados a garantir a disponibilidade da rede e a segurança dos dados. A tecnologia utilizada para coletar dados sobre os resultados das competições foi fornecida pela OMEGA, a empresa de cronometragem oficial dos Jogos Olímpicos. Mas a cidade-sede é responsável por garantir a transmissão, disponibilidade e segurança das informações. Como um atleta não pode repetir uma prova no caso de uma violação de dados, a prioridade sempre foi garantir a disponibilidade e a segurança das informações enquanto elas circulavam pelas redes em todos os momentos e em todos os locais de competição.

Foi registrado um alto nível de tráfego no Parque Olímpico, onde a OMEGA coletava dados. Além disso, houve volume de transmissão de vídeo de demanda média e outro volume de alta demanda nos centros de informações onde os dados eram processados e enviados para transmissão internacional. A disponibilidade de navegação na web também foi uma prioridade na Vila Olímpica, que abrigou os atletas durante os 19 dias de duração dos jogos. Além de fornecer disponibilidade e desempenho adequados, havia também uma preocupação com filtro de conteúdo da web para evitar inconveniências ou reclamações que pudessem afetar os participantes – um aspecto da maior importância, considerando que todos os atletas eram menores de idade.

Seleção da solução de segurança ideal

""Desenvolvemos diferentes soluções de rede para cada cidade-sede dos Jogos Olímpicos, todas com apoio dos equipamentos da Fortinet para garantir a disponibilidade, o desempenho e a segurança das informações. Implementamos 48 firewalls da próxima geração FortiGate, todos com recursos diferentes, de acordo com os requisitos e a rede de cada local. Foi lançado um processo de licitação para o serviço de interconexão e então incorporamos o equipamento de segurança da Fortinet à infraestrutura da empresa de telecomunicações", disse Linares.

A equipe de segurança de TI teve que seguir o acordo de nível de serviço (SLA) imposto pelo COI que exigia a resolução de qualquer incidente em cinco minutos, mas eles foram além e reduziram esse requisito para um minuto devido à confiabilidade da tecnologia adotada.

"A prefeitura de Buenos Aires já trabalhava com as soluções de firewall da Fortinet em dois datacenters, então a Fortinet foi uma escolha natural. Sabíamos que poderíamos encontrar uma solução completa para garantir o tráfego e a acessibilidade nos Jogos Olímpicos da Juventude; é por isso que escolhemos o pacote FortiGate completo da Fortinet, totalmente equipado com todos os seus recursos, incluindo controle de IPS, filtro web e todos os serviços associados, em cada local e nos datacenters centrais."

Os Jogos Olímpicos são um evento internacional que envolve múltiplas áreas; não existe outro evento que reúne 206 países. Os organizadores sabem que o cibercrime não é usado apenas para fins econômicos, mas também por razões políticas e ideológicas. Os riscos se multiplicam quando ao considerar os conflitos políticos e econômicos de cada um desses países.

Detalhes

Cliente: Prefeitura de Buenos Aires

Setor: Governo.

Localidade: Buenos Aires, Argentina.

Solução

FortiGate 300E-BDL, FortiGate 201E-BDL, FortiGate 1200D-BDL, FortiGate 1500D-BDL.

Impacto

- Disponibilidade 24 horas por dia, 7 dias por semana, para atender ao tráfego intenso de informações em várias redes em um evento de grande escala.
- Segurança de alto nível para prevenir incidentes de cibersegurança e garantir a integridade dos dados em uma competição esportiva internacional de elite.
- Detecção e resposta rápidas para cumprir com os SLAs de resolução de incidentes em menos de um minuto.
- Filtro de conteúdo da web para usuários menores de idade.
- Fácil gerenciamento de múltiplas redes com diferentes níveis de sofisticação e rigor.

Então, além de criar um Comitê de Segurança Federal com diferentes agências de segurança argentinas e a INTERPOL, a equipe criou vários cenários de conflito e desenvolveu soluções para cada um deles com base na tecnologia de segurança da informação da Fortinet adotada para os jogos. Cerca de 60 cenários foram criados, alguns baseados em outras experiências dos Jogos Olímpicos e outros segundo a experiência do governo ou a imaginação dos organizadores. Isso ajudou a obter detecção e resolução rápidas. Por exemplo, a equipe encontrou cinco domínios falsos semelhantes aos dos Jogos Olímpicos da Juventude, criados com a intenção de gerar golpes de phishing, que foram eliminados.

Disponibilidade para atender aos padrões mais rigorosos

"Estamos extremamente satisfeitos com os resultados alcançados. Foram 12 dias repletos de atividades com a participação recorde acima de 1 milhão de espectadores, sem incidente de cibersegurança. Conseguimos impedir, detectar e mitigar qualquer tentativa de impacto na disponibilidade ou no desempenho da rede. Com relação à administração, apesar de ter mais de 40 firewalls FortiGate de diferentes capacidades em operação, não tivemos problemas com o equipamento, apesar de termos implementado o pacote completo de segurança da Fortinet", acrescentou Linares.

A Fortinet já havia instalado o sistema de infraestrutura de segurança principal da prefeitura de Buenos Aires, facilitando muito o processo administrativo deste projeto. O fato de já conhecer as capacidades das ferramentas e sua administração facilitou todo o processo. Além disso, a Fortinet forneceu a solução mais adequada para atender às necessidades do evento, conectando cada um dos locais do evento a um datacenter central de alta disponibilidade e desempenho.

"Dedicamos um grande esforço à prevenção, análise, pesquisa e criação de uma Equipe de Resposta a Incidentes de Segurança da Computação (CSIRT - Computer Security Incident Response Team) específica para os jogos. É fundamental criar cenários de conflitos conhecidos associados a possíveis conflitos baseados na experiência profissional e política para testar a infraestrutura de segurança. Também importante é a capacidade de operar durante o evento e saber como trabalhar com rapidez e eficiência. Esse conhecimento prévio combinado ao parceiro tecnológico ideal nos permitiu detectar incidentes que já tínhamos mapeado, saber qual solução aplicar e, depois, implementá-la rapidamente para mitigar os riscos de cibersegurança", concluiu Linares.

> *"Estamos extremamente satisfeitos com os resultados alcançados. Foram 12 dias repletos de atividades com a participação recorde acima de 1 milhão de espectadores, sem incidente de cibersegurança. "*
>
> *– Gustavo Linares*

FORTINET®

www.fortinet.com