sefa ozel_CANVA

PLANEJAMENTO

# TENDÊNCIAS DE CIBERSEGURANÇA: O QUE 2022 NOS RESERVA?

**Os ataques cibernéticos explodiram durante a pandemia e, infelizmente, parece que vão continuar, já que a nova força de trabalho distribuída traz mais oportunidades que os criminosos podem aproveitar.**

**Laurence Pitt (*)**

Os cibercriminosos provavelmente continuarão explorando qualquer vulnerabilidade humana ou técnica, e capitalizando com relação aos requisitos de TI cada vez mais complexos da era de trabalho híbrido.

Aqui, examinamos quais os ataques cibernéticos podem ser as maiores ameaças para este novo ano, mas também o que os líderes de TI podem fazer para evitar que a sua organização seja vítima de um próximo ataque.

1 **Ataques contra a cadeia de abastecimento –** Em 2021, houve um aumento dramático nos ataques contra a cadeia de abastecimento: a Agência da União Europeia para Cibersegurança (ENISA) relatou um aumento de quatro vezes nos ataques.

A natureza desses ataques foi diversa, mas os criminosos buscaram cada vez mais manter como alvo as cadeias de abastecimento de softwares, permitindo que às vezes comprometessem milhares de vítimas por meio de uma única violação, ao mesmo tempo que era fornecido a eles um amplo acesso interno via sistemas confiáveis.

É muito provável que esses ataques continuem em 2022, à medida que as organizações passarão a interagir cada vez mais, não apenas com os fornecedores terceirizados, mas também com as pessoas externas. Com a ameaça exacerbada pelos desafios de proteger o novo panorama distribuído, as organizações devem pensar seriamente em como garantir que a sua cadeia de abastecimento seja a mais segura possível.

2 **Ataques de comprometimento de DNS –** Os ataques cibernéticos, como ransomware e ataques de phishing, foram manchetes em 2021, mas junto com eles, estamos vendo surgir um outro tipo de ameaça: a falsificação de DNS ou o comprometimento de cache de DNS.

Pesquisas mostram que os ataques relacionados ao DNS estão crescendo: 72% das organizações pesquisadas sofreram um ataque de DNS em 2021 e um terço delas foi vítima de comprometimento de cache de DNS. Esses são os tipos de ataques de redirecionamento, por meio dos quais um invasor cibernético viola o Sistema de Nomes de Domínio (DNS) de um usuário.

cottonbro_abre em uma nova aba ou janela_de Pexels_CANVA

Por exemplo, o usuário pensa que está visitando o site A, mas, na realidade, está sendo redirecionando para o site B. Portanto, em vez de visitar o site A, ele é direcionado para um site que se parece com o site A, mas este é falso. O usuário ainda pode ser direcionado para o site pretendido, mas seguirá por outro caminho onde todos os dados inseridos poderão ser coletados.

3 **Confiança zero (Zero Trust) –** Um método de proteger os valiosos sistemas e dados das organizações é implementar uma política Zero Trust. Muitas organizações já estão familiarizadas com o conceito, mas em 2022 a política Zero Trust ganhará mais impulso entre as organizações.

Zero Trust desempenha um papel importante no desafio de proteger a cadeia de abastecimento, por exemplo, porque depende de não confiar em ninguém com acesso aos seus dados ou à sua rede até que se qualifique como "confiável" novamente, mesmo que apenas se confie nesse ponto por um determinado tempo ou para uma atividade em particular.

Zero Trust também pode mitigar algumas das ameaças associadas ao trabalho remoto, incluindo a prevenção do acesso a sistemas e a dados por meio de dispositivos inseguros rodando em uma mesma rede, que um dispositivo remoto corporativo. Na verdade, o Zero Trust cria um casulo em torno das atividades dos funcionários para garantir que qualquer ataque cibernético em potencial não se espalhe além dessa instância.

4 **Segurança desde o design –** Sempre que as pessoas tomam decisões sobre segurança, elas devem considerar a criação de segurança do zero. Há duas razões para isso. A primeira é que é muito mais fácil projetar uma segurança eficaz e onipresente no início de qualquer implementação, em vez de tentar aplicá-la quando todas as decisões tiverem sido tomadas.

O segundo motivo é que às vezes a adição de camadas de segurança pode afetar outras coisas, como a experiência do usuário. Por exemplo, a aplicação de filtros projetados para impedir que as pessoas visitem determinados sites, na verdade, pode impedi-las de acessar sites de negócios perfeitamente válidos.

É por isso, também, que às vezes a segurança tem a reputação de ser um departamento que diz:"não". Talvez as decisões de design tenham sido feitas e, em seguida, a proteção tenha sido adicionada, deixando a equipe de segurança sem opção a não ser dizer "não" ao detectar vulnerabilidades.

Além disso, a relevância da segurança deve ser claramente comunicada aos funcionários e às partes interessadas. Não deve ser algo feito de maneira inconsistente. Deve ser comunicada com muita clareza, de forma que as mudanças estejam ocorrendo no ambiente de TI. É um desafio cultural e tecnológico.

5 **Ssshhh ...** protegendo a rede em silêncio - A era do trabalho híbrido está chegando. Dados do governo do Reino Unido mostram que 85% das pessoas desejam aplicar a abordagem híbrida para trabalhar em casa e no escritório, futuramente. Portanto, embora haja a tendência de maior retorno à vida no escritório em 2022, os mesmos níveis de atividades provavelmente não serão observados como antes da pandemia.

LagartoFilm_CANVA

Uma ocupação menor e padrões de trabalho menos previsíveis serão possíveis no futuro. Com muitos escritórios operando com capacidade e atividades na rede reduzidas e com uma menor pressão, agora pode ser uma grande oportunidade de realizar um benchmark do ambiente, detectando quaisquer elementos potenciais que não deveriam estar lá e entendendo onde pode haver riscos.

Pense nos dispositivos de rede que foram implementados - eles estão fazendo seu trabalho, porém representam algum risco? Talvez as TVs na sala de conferência, que podem se conectar à rede Wi-Fi corporativa ou até mesmo via Bluetooth?

É possível haver todos os tipos de dispositivos em uma rede corporativa, que poderiam ser melhor configurados com relação à segurança, mas isso não aconteceu no passado porque ninguém teve tempo ou sempre foi muito difícil devido a um grande tráfego de rede com um enorme número de pessoas no edifício.

As organizações estão buscando a tecnologia da Internet das Coisas (IoT), para ajudá-las a manter um ambiente confortável no escritório, mais seguro e com eficiência energética. Agora, é o momento perfeito para otimização da segurança desses e de quaisquer outros dispositivos na rede até 2022.

**(*) - É Estrategista de Segurança Global da Juniper Networks (https://www.juniper.net/br/pt/).**