RANSOMWARE: Proteger é uma prioridade

Sabemos que o **cibercrime** tem aumentado de ano para ano, mas nunca foi tão frequente como neste periodo de pandemia. A **cibersegurança** está a ser afetada porque muitos estão agora a trabalhar de casa e a digitalização tornou-se ainda mais importante: onde há mais dispositivos e pessoas conetadas, existem mais problemas de segurança. O **ransomware** representa quase a totalidade das ameaças que temos hoje em dia, e foi uma das ameaças que mais aumentou, mais de 60% em 2020, e é um grande problema. O **Ransomware** é o tipo de malware usado para extorquir dinheiro, pois mantém os dados ou dispositivo como refém até ser pago o resgate .

QUEM SÃO OS ALVOS?

Recentemente assistimos a um ataque massivo causado por este vírus nas Energias de Portugal (EDP). Apesar de não interferir no fornecimento da energia, estes dados da empresa estavam encriptados e na posse destes hackers que, alegadamente, exigiram um resgate na ordem dos 10 milhões de euros, com um prazo de 20 dias. Mas não se iluda quando pensa que quanto menor for a empresa menor é o interesse por parte dos hackers. Na verdade, são muito atrativas para este tipo de ataques. Mais de 70% dos ataques têm como alvo as **PME** , com sistemas de segurança mais fracos e menores recursos financeiros. Uma empresa como a EDP investe milhões em cibersegurança, tem sistemas redundantes e consegue repôr rápidamente as operações. A maior parte das **PME** não tem possibilidades de investir desta forma, estão mais vulneráveis, menos defendidas e quando são atacadas o impacto pode ter efeitos devastadores nas operações, expondo dados pessoais e de clientes e ditar mesmo o fim do negócio.

A SEGURANÇA É UMA PRIORIDADE

A segurança é sem dúvida uma prioridade, principalmente para as **PME**. Os ataques às **PME** são tipicamente feitos utilizando ferramentas que fazem o scan automáticamente na Internet à procura de vulnerabilidades do IT. A **cibersegurança** nos dias de hoje tornou-se numa necessidade e já não passa por uma opção. A **Covid-19** pode ser um incentivo para estes ataques. A maioria das **PME** estava despreparada para iniciar o **teletrabalho**, vendo-se obrigada a adaptar-se de qualquer forma, VPN feita à pressa e sem segurança de rede, workstations sem proteção adequada. A área digital da empresa aumentou brutalmente passando, por exemplo de um escritório para 20 funcionários para 20 escritórios, um em casa de cada colaborador. Ninguém estava preparado para isto. Tudo isto fez com que os ataques viessem a aumentar.

Como é consegue manter a PME protegida deste tipo de ciberataques? Nos dias de hoje os cibercriminosos desenvolvem e combinam táticas de ataque com o objetivo de garantir o máximo dano e por sua vez, o máximo sucesso financeiro. A maior parte dos ataques são automatizados, acontecem em vários sitios ao mesmo tempo, surgem de emails ou websites fraudulentos. Por esta razão, a **cibersegurança** é uma prioridade, numa altura em que a pandemia transformou a forma como as pessoas trabalham, e que em muitos casos será o novo habitual. Assim, para combater este tipo de ataques modernos é essencial uma proteção em camadas com tecnologias com uma base de inteligência. Uma camada de defesa não é suficiente. A **base de inteligência** destas proteções deteta os ataques antecipadamente, deteta atividade suspeita que esteja a acontecer em qualquer lugar no mundo e toma decisões automatizadas, melhora a capacidade de deteção e solução dos problemas.

Proteção em camadas

Mas para combater estes ataques que camadas de segurança são necessárias e acima de tudo suficientes? A segurança **endpoint** e a **segurança de rede** são essenciais. .

Segurança EndPoint

Se pensarmos no caso do **Ransomware** o ataque começa sempre no mesmo local, na workstation. Portanto, a primeira camada de proteção concentra-se precisamente em proteger o desktop, laptop ou dispositivo móvel do que vem de fora. A segurança endpoint evoluiu do tradicional software antivírus para a **proteção endpoint** moderna mais abrangente e à base de inteligência, que verifica todos os ficheiros e ligações e garante que não contêm ficheiros maliciosos nem que visitemos páginas fraudulentas. Uma proteção endpoint em tempo-real, contra ameaças provenientes de e-mails, browsers, ficheiros, URLs, anúncios, aplicações, entre outros, para prevenir ataques, detetar atividade maliciosa e facultar capacidade instantâneas de remediação.

Segurança de rede

Enquanto a camada anterior é a muralha que analisa todas as informações que vêm de fora, esta pode dizer-se que protege o centro da cidade, neste caso o servidor e o storage da empresa, o ponto mais crucial. Uma solução de segurança de rede situa-se no meio das ligações (ex. workstation-datacenter) e no ponto de entrada e saida de rede. A **segurança de rede** concentra-se em monitorizar determinados sinais na rede tais como o fluxo de tráfego, origem, proveniência e constituição desse tráfego. O facto de o fazer sem acesso a um sistema operativo e os seus sinais faz com que, muitas vezes, consiga detetar ameaças silenciosas tais como ameaças avançadas, vírus de ransomware que não se deixaram detetar nos endpoints, tentativas de scan externos, ameaças web, entre outros. Para impedir as ameaças de entrarem na rede, incluí:

- **Monitorização de tráfego:** Os sistemas analisam e compara o tráfego de rede em relação ao comportamento padrão. Inclui a análise da origem e destino;
- **Inspeção de conteúdo e forma do tráfego:** Capacidade de deteção de código

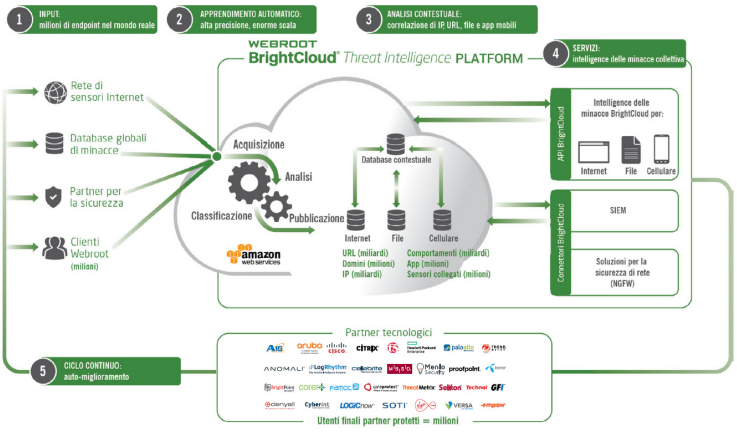
malicioso, Scans de Rede, SQL Injection, Cross Site Scripting, tentativa de abertura de conexão, instruções, entre outras;

- **Inspeção de Sessões:** Capacidade de validar os utilizadores que se ligam e de garantir isolamento de sessões;
- **Encriptação de Tráfego**: Capacidade dos sistemas de encriptarem o tráfego que circula na sua rede.

AS NOSSAS SOLUÇÕES WEBROOT E ENDIAN

Solução Endpoint Webroot

A **Webroot Secure Anywhere** faz deteção e proteção em tempo real. É capaz de neutralizar os softwares maliciosos e as ameaças tipo zero -day a partir do momento em que o ataque é detetado. Usa arquitectura baseada na cloud, dispensando instalação ou atualizações de assinaturas ou definições. Assim o agente instalado é leve e muito eficiente. Para além disso a **EndPoint Protection** utiliza uma aproximação de Raw scanning, que combinada com outras técnicas, significa que trabalha mais rapidamente que os outros antivírus. A estratégia Webroot " nova geração" é mais eficaz e fiável que os antivírus tradicionais. O **Webroot SecureAnywhere** disponibiliza camadas de proteção adicionais através da plataforma de inteligência de ameaças **BrightCloud**, que cruza dezenas de milhões de informações, em todo o mundo sobre ocorrências de malware e aplicações duvidosas, monitorizando biliões de endereços IP e URLs todos os dias. E aqui entra a deteção de ameaças e a resposta automatizada. Uma solução que não só utiliza **inteligência artificial** (IA) e **machine learning** (ML) mas também as utiliza para automatizar tarefas e ser mais rápida e eficaz e não só trava as ameaças mas prevê e previne proativamente.



Estrutura da plataforma de inteligência Webroot BrightCloud e parceiros tecnológicos

Solução de segurança de rede Endian

A **Endian** é uma empresa especialista em soluções de segurança de rede para empresas, possuindo também soluções para a indústria. Uma parte importante dos seus produtos é a gama "**Unified Threat Management (UTM)**", atualmente muito utilizada e ainda com maiores vendas face à mudança que estamos a assistir no nosso ambiente de trabalho empresarial, o remote smart working. De facto, esta nova forma de trabalhar para além das óbvias dificuldades de infraestruturas colocou inumeras questões relativamente à

segurança das ligações de casa e empresa. A **endian UTM** permite configurar uma coneção **VPN** de casa à empresa, em que os utilizadores podem aceder de forma segura aos ficheiros e aplicações a partir de casa, evitando infiltrações de vírus. Esta **UTM** é ideal para as **pequenas e médias empresas** abaixo indicadas e que precisem de atualizações de constantes, suporte comercial e um sistema fácil que possam instalar e esquecer.

- **Quem precisa de uma segurança de rede UTM?**

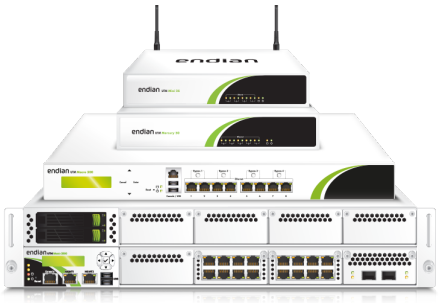
Empresas com ligações entre postos e pelo menos um servidor/ storage comum / rede interna, partilha de aplicações e dados. Precisam de segurança avançada com camadas (statefull inspection firewall, VPN, antivírus, anti spam, filtro web e de conteúdo) de forma a proteger as ligações nos seus pontos de entrada e saída.

Empresas sediadas em vários locais - com troca de dados entre filiais e sede, precisam de segurança integrada com statefull inspection firewall, VPN, gateway anti-vírus, antispam, filtro web e conteúdo e ainda hotspot, num único produto.

Empresas com websites alojados em webservers - configuração automática, filtros, análise e correlação de dados sem afetar o desempenho da rede.

- **Features das soluções de segurança de rede:**

Monitorização de Tráfego: IDS, IPS, Anti-Beaconing
Inspeção de Conteúdo e forma: Email Security, Antivirus (Filtro de Pacotes), WAF
Inspeção de Sessões + Encriptação: VPN, Autenticação Segura, Encriptação de Tráfego



UTM por hardware , software ou virtuais : Endian Mini 10 e 25, Mercury 50, 100 , Macro 250

ARRISCAR O FUTURO DA EMPRESA POR FALTA DESTAS SEGURANÇAS? NÃO COMPENSA

Com o desenvolvimento tecnológico, a cibersegurança para as **pequenas e médias empresas** deixou de ser um luxo e neste momento é considerada uma necessidade prioritária. Com os ataques informáticos cada vez mais frequentes, têm vindo a desenvolver equipamentos e softwares capazes de impedir que os mesmos causem estragos nos sistemas, fáceis de operar e com preços acessíveis. Os ataques de **ransomware** deixam os sistemas muito afetados e não compensa para as empresas arriscar a sustentabilidade dos seus negócios. Não corra esse risco e conheça as nossas soluções **Webroot** e **Endian**, intuitivas e inteligentes que permitem uma cibersegurança eficaz , em especial para as **PME** , a maior parte do nosso tecido empresarial, a um preço que podem pagar.

Contacte-nos