SOLUÇÕES DE SEGURANÇA DE REDE
INDÚSTRIAS LOGÍSTICAS E FABRICO

PORQUE É QUE O SETOR INDUSTRIAL PRECISA DE SEGURANÇA DE REDE?

A Indústria 4.0, também conhecida por industry IoT (industrial internet of things), é uma oportunidade tremenda para empresas ligadas ao ramo industrial, em várias vertentes:

1. Melhoria da produtividade, graças à automatização dos processos, manutenção preventiva com menos tempo perdido por causa de avarias nos equipamentos industriais;

2. Melhoria no processo de fabrico e produção mais eficaz graças aos diagnósticos em tempo real;

3. Economias e benefícios ecológicos graças à maior eficiência energética;

4. Controlo à distância dos parâmetros do estado de um produto entre outras.

Mas esta gestão inteligente das fábricas a que temos vindo a assistir, também aumenta exponencialmente os riscos de ataques provenientes da Internet: a IoT industrial alarga o leque de novas vulnerabilidades que os cibercriminosos podem explorar. Com a superfície de ataque mais ampla e uma integração alargada de rede, existem mais dispositivos conectados, mais interações máquina a máquina, mais transferências de dados via Internet para controlar as operações das máquinas, sinalizar falhas e alertar necessidades de manutenção. Com estas novas otimizações existem, por isso, novos pontos de entrada para os cibercriminosos.

No setor industrial, agora com grande parte da estrutura fabril ligada à Internet, a Segurança de Rede é indispensável para permitir a manutenção remota e impedir o roubo de dados, apropriação indevida de segredos industriais e manipulação de máquinas. As consequências geradas por estes ataques informáticos diferem em muito dos pequenos escritórios, na medida em que a perda de dados ou paragens na produção podem ter um efeito devastador, conduzir a graves perdas económicas e são uma preocupação constante para estas empresas industriais.

É necessário prevenir estes ataques aos sistemas de informação das instalações industriais antes de poderem paralisar a fábrica. Proteger as fábricas de ameaças internas, externas e de fornecedores é assim indispensável.

A QUE TIPO DE AMEAÇAS ESTÁ O SETOR SUJEITO?

Os ciberataques a infraestruturas industriais estão na ordem do dia. Todos os anos, os cibercriminosos desenvolvem ameaças direcionadas cada vez mais avançadas. Apesar de não ser mencionado tantas vezes, o setor Industrial não fica indiferente a este tipo de ameaças. Alguns cibercriminosos ocupam-se a analisar de perto as características de negócios industriais e obtêm, assim, acesso a uma grande quantidade de informação sobre as suas redes tecnológicas.

1. **Os ataques de Ransomware**, mais especificamente contra sistemas de controlo industrial ICS, são cada vez mais direcionados e sofisticados. Com a pandemia, esta ameaça tem vindo a agravar-se de forma significativa, uma vez que as redes industriais se tornaram mais vulneráveis, devido aos limites impostos ao trabalho no local, bem como aos espaços de trabalho pessoais dos colaboradores.

Da mesma forma que uma PME sofre ataques automatizados de Ransomware, a fábrica sofre os mesmos ataques e das mesmas formas. A diferença é que uma fábrica tem menos computadores do que uma empresa por trabalhador. Isto poderá querer dizer que é menos provável uma fábrica ser atacada do que uma pequena empresa, em virtude da exposição ser menor. Por outro lado, os utilizadores dos computadores das fábricas são normalmente administrativos ou trabalhadores especializados, que têm menos conhecimentos em tecnologia, estando mais vulneráveis aos ataques de phishing. Através destes ataques de phishing, os cibercriminosos roubam palavras-passe e contas previligiadas, permitindo o acesso à informação mais crítica das empresas.

Em termos de pontos de entrada, a entrada de Phishing nas fábricas, é feita através destes computadores (browser ou e-mail) podendo, em caso de ataques mais sofisticados, ser feita através do update de aplicações pelo servidor ou pelas próprias máquinas de produção, embora seja mais raro.

Existem algumas formas das indústrias se defenderem do Ransomware. **A Webroot Security Anywhere**, é uma solução de **Endpoint Security** que pode impedir a entrada destas ameaças nos PCs e Servidores, através da download de ficheiros. Pode também evitar os ataques de phishing de browser através do Web filtering.

Quando nos referimos a ameaças de phishing através de email ou queremos prevenir que os cibercriminosos comuniquem com as máquinas de rede e sejam dadas informações às mesmas que possam provocar paragens ou avarias, deve-se optar pelas soluções Endian IOT. Nas redes industriais a quantidade de dados transacionados é menor que nas pequenas e médias empresas.

Embora as **Endian 4i Edge da linha IOT** processem menos informação do que as UTMs normais da Endian, oferecem uma segurança de rede potente incluindo segmentação de rede, controlo firewall completo, IPS/IDS, sistema de deteção e intrusão com a tecnologia Deep Packet e filtering layer -7. Têm, ainda, características mais ajustadas e fundamentais para muitas empresas industriais como a sua robustez, capacidade de suportar temperaturas mais adversas ou com grandes variações para instalações mais robustas. Suportam, também, múltiplas plataformas de Internet e conectividade SCADA, incluindo Ethernet, Wi-Fi, 3G/4G e série (RS-232/485).

Para além deste tipo de ameaças que é mais focado na retenção de dados para posterior pedido de resgate, muitas vezes neste setor os cibercriminosos direcionam os seus ataques para as máquinas industriais em si, alterando programações, inserindo avarias ou parando mesmo toda a produção. Estes ataques afetam em muito as empresas industriais, não só devido ao tempo de paragem a que são obrigadas, mas também pelos prejuízos que têm ao nível de matéria-prima.

2.

O **roubo de dados interno** é uma ameaça pouco falada, no entanto relativamente comum nestes casos. Na fábrica, a proteção de invenções, desenhos industriais, planos, patentes e outros tipos de propriedade intelectual é fundamental. É importante proteger estes ativos e por isso, para além do acesso restrito a esta informação, precisamos de ser capazes de verificar os ficheiros que entram e saem e monitorar aqueles com informação confidencial. O roubo destes dados pode causar à fábrica prejuízos avultados. Para responder às necessidades destas organizações, pode-se utilizar a solução simples e económica do **Device Lock DLP** para impedir o roubo informação interna. Esta solução impede que os dados sejam retirados dos endpoints, portáteis empresariais Windows ou Mac, desktops ou sessões e aplicações virtualizadas Windows.

3.

Os ataques a partir de firmware são outras das ameaças a que este setor está sujeito. As fábricas têm diferentes máquinas de produção, com diferentes fabricantes. Estas máquinas poderão estar ligadas a uma cloud do fabricante, onde o mesmo atualiza o software próprio de cada máquina. Se o fabricante for atacado, é possível enviar, em vez de atualizações legítimas, vírus, ransomware ou outro tipo de instruções maliciosas para as máquinas de produção, perturbando o seu funcionamento. É um ataque semelhante aquando os sistemas Windows numa empresa pequena ou média empresa, procedem a atualizações que não são legítimas.

Não existe maneira de evitar diretamente este tipo de ataques, uma vez que não controlamos a infraestrutura do fabricante nem há maneira de validar se as atualizações são legitimas. Contudo, a segurança de rede tem um papel fundamental porque pode impedir as máquinas comprometidas de comunicarem com exterior e pedirem instruções evitando assim que o ataque se alastre para outras máquinas, através do filtro da rede. A Endian é essencial para limitar os danos deste ataque que é potencialmente muito perigoso.

No seguimento do artigo iremos abordar mais detalhadamente as soluções Webroot e Endian, focando-nos mais especificamente nas suas características e nas vantagens que as mesmas trazem para a segurança das indústrias.

Apostar em segurança de rede neste setor é muito mais que proteger apenas os computadores que estão na parte administrativa, é proteger todo um sistema de produção, de que estas empresas industriais dependem. Os sistemas ficam protegidos de ameaças, não há retenção de dados privados por terceiros e principalmente, a produção não é afetada, não havendo desperdício de recursos. Esta é uma altura de transformação das indústrias e o IOT é uma forma de aumentar a produção ao ter os sistemas ligados em rede, o que ajuda a prevenir quebras de produção causadas por avarias.

WEBROOT SECURE ANYWHERE ENDPOINT PROTECTION

O Webroot desenvolveu uma solução de segurança informática no âmbito cloud que distribui a nível mundial. O Webroot EndPoint Protection oferece uma abordagem revolucionária à proteção dos endpoint contra vírus e malware.

A solução combina a tecnologia inovadora Webroot com reconhecimento de comportamentos e de padrões de ficheiros, com a potência da cloud para bloquear ameaças.

Esta é uma solução bastante completa, totalmente baseada na cloud, o que faz com que as definições não sejam descarregadas no endpoint e, por isso, está sempre atualizado.

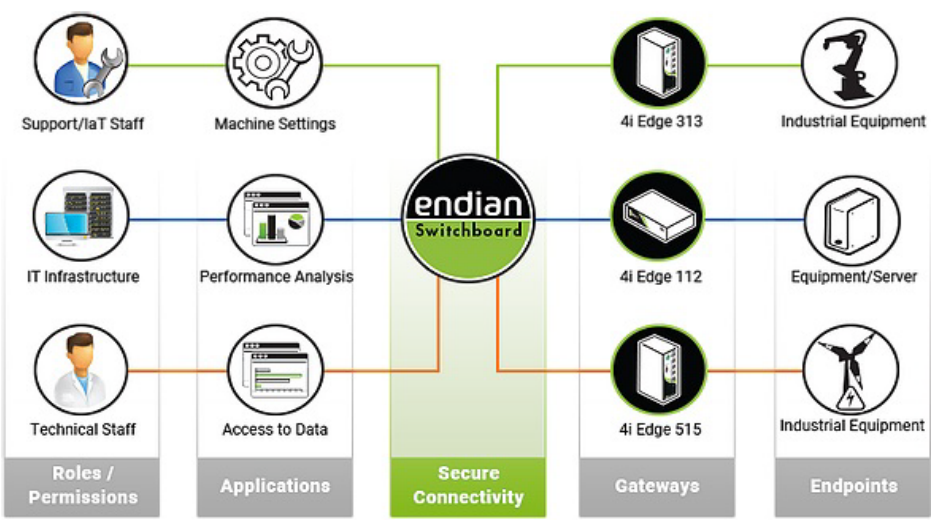
A incorporação da Webroot Intelligence Network, a maior rede mundial de deteção de malware que integra milhares de informações provenientes de inúmeras fontes (clientes, laboratórios de teste, dados de inteligência partilhados por fabricantes de segurança), faz da Webroot uma solução completa e muito eficaz.

SOLUÇÃO ENDIAN CONNECT

A **Endian** é líder no desenvolvimento de soluções de segurança fáceis de utilizar há mais de 15 ano. Tem soluções segurança e manutenção remota para a indústria fundamentais para a transformação digital de sucesso nestas empresas, focadas em evitar estas ameaças tão presentes nos dias de hoje.

A resposta a estes desafios é feita através da plataforma **Endian Connect**, composta por um software Switchboard que permite monitorizar e visualizar em tempo real (dashboard), com total segurança, os dispositivos ligados à rede. Esta plataforma é também composta por uma firewall industrial: a **4i Edge**. É devido a esta firewall industrial que é possível uma conexão segura entre máquinas, desde a transmissão dos dados coletados no terreno à distribuição granular dos direitos de acesso aos utilizadores em conformidade com a legislação, privacidade e a proteção do sigilo industrial. A solução Endian Connect junta tudo isto numa consola centralizada com um dashboard intuitivo e mapa de geolocalização.

A **Endian Connect** "faz frente" aos crescentes perigos da indústria 4.0. Protege a comunicação industrial e garante a comunicação à distância das máquinas permitindo associar um número ilimitado de endpoints através de uma Internet segura – independentemente do sistema operativo.



SOLUÇÃO 4I EDGE

A conexão das máquinas industriais à internet cada vez é mais comum e torna necessária a proteção dos dados de ciberataques, especialmente na fase de transmissão em que não devem ser roubados ou manipulados.

O amplo conjunto de funcionalidades de controlo e segurança contra as ciberameaças, incluindo funcionalidades de firewall, filtram o tráfego perigoso e protege o fluxo de dados. Estas gateways da Endian têm ainda sistema de deteção e encriptação (IPS/IDS), garantindo a máxima proteção de dados e sistemas.

A conexão VPN entre a gateway Endian 4i e a plataforma switchboard é encriptada, para que os dados possam transitar com segurança e controlo em qualquer momento. Considerando a diversidade do mundo IoT industrial, estas soluções suportam protocolos heterogéneos: do tradicional http, https, VNC,RDP e Telnet, aos específicos da indústria Siemens S7, Modbus e OPCUA. A Endian 4i Edge permite ainda a manutenção das máquinas à distância, associar um número ilimitado de Endpoints através de uma ligação Internet segura e ser utilizado para proteger e conectar máquinas ou toda a rede.

As Gateways Industriais Endian 4i são utilizadas para ligar os sistemas no terreno ao Switchboard central, referido anteriormente. A instalação destas gateways é muito intuitiva, destacando-se a funcionalidade Plug&Connect, que permite a configuração simples e rápida de inúmeros dispositivos à ferramenta de gestão central. Para o fazer, o administrador pré-configura facilmente todos os dispositivos gateway.

De seguida, basta ligar a gateway remota a uma rede. Estes equipamentos permitem uma interoperacionalidade com a estrutura existente, pois a APP da Endian permite às empresas industriais integrarem todas as funções do painel de comandos em plataformas pré-existentes, por exemplo no portal de suporte dos parceiros.

Em suma, é um software de manutenção de gestão remota que permite gerir um elevado número de conexões. A fórmula "tudo incluído" permite optar por uma única tecnologia de proteção de ameaças e resolução de problemáticas múltiplas, baixando o custo de gestão e de funcionamento. Os responsáveis pela manutenção e suporte podem realizar grande parte da atividade acedendo remotamente à máquina sem deslocações, com notável otimização de recursos.

SERVIÇO VPN

GESTÃO CENTRALIZADA CONNECT SWITCHBOARD

CONECTIVIDADE ILIMITADA

LIGAÇÃO REMOTA IOT

4i EDGE 515

Firewall Throughput
120 Mbps

VPN Throughput
30 Mbps

5 PORTAS DE REDE

4i EDGE 112

Firewall Throughput
120 Mbps

VPN Throughput
30 Mbps

2 PORTAS DE REDE

4i EDGE X

Firewall Throughput
3 Gbps

VPN Throughput
250 Mbps

Ips Throughput
300 Mbps

Os Endian Edge são uma solução industrial de desktop poderosa e escalonável. Todos os recursos incluídos no produto garantem que suas redes industriais remotas tenham os mais altos níveis de disponibilidade. São equipamentos robustos, bem preparados para aguentar as temperaturas variáveis e extremas que muitas vezes se verificam nas indústrias.

A indústria 4.0, a transformação digital e a conformidade com o GDPR são atualmente os maiores desafios para as empresas industriais portuguesas. No entanto, esta nova realidade abre também uma janela de oportunidades para a implementação de novas tecnologias, como a Industrial IoT e inteligência artificial para aumentar a eficiência, melhorar a produtividade, qualidade de serviço, competitividade. Tal como as pequenas e médias empresas, as indústrias devem também estar bem protegidas das ameaças de rede, não desvalorizando as mesmas.

Na Minitel, temos uma equipa especializada pronta a analisar todas as situações e aconselhar a melhor solução possível. Contacte-nos através de info@minitel.pt para que possamos ajudar.

CONTACTOS

NEXT@MINITEL.PT

WWW-MINITELNEXT.COM

21 381 09 00