eurotux

MOVING BUSINESS FORWARD

Eurotux

QUAL O PAPEL DA CIBERSEGURANÇA NA SUA ORGANIZAÇÃO?

No mundo tecnologicamente avançado de hoje, em que as empresas dependem cada vez mais de infraestruturas e dados digitais, a importância da cibersegurança não pode ser subestimada. Com a proliferação de ciberameaças sofisticadas, tornou-se imperativo para as organizações dar prioridade e investir em medidas robustas de cibersegurança.

POR QUE RAZÃO PRECISO DE UMA BOA POLÍTICA DE CIBERSEGURANÇA?

PROTEÇÃO DE DADOS SENSÍVEIS

Uma das principais razões pelas quais a cibersegurança é vital para as empresas é a proteção de dados sensíveis. As organizações lidam com informação confidencial, dados pessoais e outros, incluindo dados de clientes, registos financeiros, segredos comerciais e propriedade intelectual. Um ciberataque bem sucedido pode levar à violação de dados ou à destruição de sistemas, resultando em consequências graves, como perdas financeiras, danos na reputação, responsabilidades legais e perda de confiança dos clientes.

GARANTIA DA CONTINUIDADE DO NEGÓCIO

As ciberameaças, como por exemplo ataques de ransomware, podem paralisar as operações de uma organização. Imagine as consequências de uma interrupção prolongada do sistema, de uma perda de dados críticos ou de uma incapacidade de aceder a recursos essenciais para assegurar o funcionamento da organização.

MITIGAÇÃO DE PERDAS FINANCEIRAS

Os ataques cibernéticos têm o potencial de infligir perdas financeiras substanciais às empresas. As consequências de um ataque bem sucedido envolvem frequentemente custos de correção, despesas legais, indemnização de clientes e multas regulamentares. Além disso, as empresas podem sofrer um declínio nas receitas devido a danos na reputação, perda de confiança dos clientes ou queda do preço das ações. Ao implementar proativamente medidas de cibersegurança, as organizações podem reduzir a probabilidade destas perdas associadas a este tipo de incidentes.

GARANTIA DE CONFORMIDADE COM OS REGULAMENTOS

Nos últimos anos, os governos introduziram regulamentos rigorosos de proteção de dados para salvaguardar a privacidade dos indivíduos e promover a confiança nas transações digitais. O não cumprimento destes regulamentos, como o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia ou a Lei de Privacidade do Consumidor da Califórnia (CCPA), pode levar a sanções severas. Ao dar prioridade à cibersegurança, as empresas podem garantir o cumprimento dos requisitos regulamentares, evitar consequências legais e demonstrar o seu empenho na proteção dos dados dos clientes.

PRESERVAÇÃO DA REPUTAÇÃO E A CONFIANÇA DOS CLIENTES

A reputação e a confiança dos clientes são ativos inestimáveis de qualquer empresa. Uma única violação de dados pode manchar a imagem de uma empresa e corroer a confiança dos clientes, levando a uma perda de clientela e de quota de mercado. Medidas proativas de cibersegurança e uma comunicação transparente sobre as práticas de proteção de dados ajudam as empresas a criar confiança junto dos seus clientes. A demonstração de um compromisso com a cibersegurança promove a lealdade e a melhoria da reputação da organização como guardiã responsável de informações sensíveis.

COMBATE À EVOLUÇÃO DAS CIBERAMEAÇAS

As ciberameaças estão em constante evolução, com os atacantes a empregarem técnicas cada vez mais sofisticadas para explorar vulnerabilidades. As empresas precisam de se manter um passo à frente, melhorando continuamente as suas capacidades de cibersegurança. Isto implica investir em soluções de segurança avançadas, efetuar avaliações de risco regulares, formar os colaboradores sobre as melhores práticas de cibersegurança e manter-se informado sobre o mais recente cenário de ameaças.

ESTATÍSTICAS DE CIBERATAQUES A EMPRESAS

45% - A Gartner prevê que até 2025, quase metade das empresas a nível global vão sofrer um ataque na sua supply chain.

8 biliões - Prevê-se que o custo do cibercrime atinja os 8 biliões de dólares em 2023 e cresça para 10,5 biliões em 2025, de acordo com o "2022 Official Cybercrime Report" da Cybersecurity Ventures.

52 mil milhões de dólares – Valor em perdas por fraude de identidade em 2022, de acordo com o "2022 Identity Fraud Study " da Javelin Strategy & Research.

277 dias – Tempo médio que as equipas de segurança demoram a identificar e conter uma violação de dados, de acordo com o "Cost of a Data Breach 2022", um relatório publicado pela IBM e pelo Ponemon Institute.

150 mil dólares - De acordo com o relatório da IBM "Cost of a Data Breach 2022", as violações de dados que envolvem credenciais perdidas ou roubadas demoram mais tempo a identificar e custam mais 150 000 dólares do que a média das violações de dados.

10TB – Dados roubados por mês entre maio de 2021 e junho de 2022, de acordo com o Relatório da European Union Agency for Cibersecurity; dados referentes a União Europeia, Reino Unido e Estados Unidos da América.

94.2% - Percentagem de casos de ataques de ransomware em que não se sabe se as organizações pagaram ou não o resgate.

ABORDAGENS DENTRO DA EMPRESA

Com o crescente número de ciberameaças, a segurança da informação tornou-se uma preocupação primordial para as empresas em todo o mundo. Para a proteção eficaz de dados sensíveis e para garantir a continuidade do negócio, é essencial adotar uma abordagem em camadas de cibersegurança.

CAMADA DE PROTEÇÃO DE PERÍMETRO

A primeira linha de defesa em qualquer sistema de segurança é a camada de proteção de perímetro. Essa camada envolve a utilização de firewalls, gateways de email, gateways de internet e outros dispositivos de segurança que atuam como uma barreira entre a rede interna da empresa e a internet. Todos em conjunto ajudam a filtrar e bloquear ameaças externas, como malware, vírus e ataques de hacking.

CAMADA DE AUTENTICAÇÃO E IDENTIFICAÇÃO

A autenticação é outra camada crucial de cibersegurança que garante que apenas utilizadores autorizados têm acesso aos recursos da empresa. Envolve a implementação de passwords fortes, autenticação em dois fatores (2FA) e tecnologias de autenticação biométrica, como impressões digitais ou reconhecimento facial. Ao exigir várias formas de identificação, essa camada dificulta o acesso não autorizado a informações confidenciais.

CAMADA DE SEGURANÇA DE REDE

Uma boa cibersegurança envolve a segmentação da rede em diferentes zonas de segurança. Isso significa dividir a rede em sub-redes, cada uma com suas próprias políticas de segurança e restrições de acesso. Essa abordagem permite controlar e monitorizar melhor o tráfego interno, facilitando a deteção de atividades suspeitas ou anormais.

CAMADA DE SEGURANÇA DE DADOS

A segurança dos dados é uma das maiores preocupações para as empresas. Para proteger efetivamente seus dados, é essencial implementar medidas como criptografia de dados, backups regulares e políticas de acesso restrito aos dados sensíveis. Além disso, é fundamental educar os funcionários sobre boas práticas de cibersegurança e promover a consciencialização sobre a importância da proteção de dados.

CAMADA DE MONITORIZAÇÃO E RESPOSTA A INCIDENTES

Mesmo com todas as medidas de segurança implementadas, é importante ter em vigor um sistema de monitorização e resposta a incidentes. Monitorizar a rede regularmente em busca de atividades suspeitas ou anormais é essencial para identificar ameaças em potencial. Ter um plano de resposta a incidentes ajuda a mitigar o impacto de um ataque e a minimizar a perda de dados.

CONSEQUÊNCIAS DE CIBERATAQUES BEM-SUCEDIDOS

PERDAS FINANCEIRAS

DANOS NA REPUTAÇÃO DA EMPRESA

PERDA DE CONFIANÇA DOS CLIENTES

DADOS COMPROMETIDOS

INDISPONIBILIDADE DE SISTEMAS

OPERAÇÕES COMERCIAIS INTERROMPIDAS

SEGURANÇA COMO UM SERVIÇO – O QUE É E QUAIS AS VANTAGENS?

Um serviço de Security as a Service (SecaaS) é uma abordagem em que uma empresa entrega os seus serviços de segurança na forma de outsourcing a um prestador de serviços especializado, como a Eurotux. Em vez de investir em recursos internos e infraestrutura de segurança, as empresas optam por contratar serviços de segurança personalizados. Então, quais as principais vantagens?

ESPECIALIZAÇÃO E EXPERIÊNCIA

Os prestadores deste tipo de soluções têm conhecimentos aprofundados em cibersegurança e estão atualizados para fazer frente às últimas tendências e ameaças. Eles contam com equipas de especialistas dedicados, com um leque de competências variadas, oferecendo assim um alto nível de experiência.

REDUÇÃO DE CUSTOS

Contratar uma empresa para assegurar os serviços de cibersegurança torna-se mais económico do que investir em recursos internos. Os custos de aquisição e manutenção de hardware e software de segurança, formações e contratação de especialistas podem ser evitados com a externalização dos serviços de segurança.

ESCALABILIDADE E FLEXIBILIDADE

Estes serviços podem ser facilmente escalados para atender às necessidades de uma empresa em crescimento. Empresas como a Eurotux têm a capacidade de ajustar recursos e fornecer soluções personalizadas, em linha com as alterações das necessidades e com os desafios do negócio dos clientes.

MONITORIZAÇÃO E ALERTAS EM TEMPO REAL

Os prestadores de serviços de cibersegurança oferecem monitorização 24 horas por dia, 7 dias por semana, para detetar e responder a ameaças em tempo real. Este cenário ajuda a minimizar o tempo de resposta a incidentes e evitar danos significativos aos sistemas e dados da empresa.

ACESSO A TECNOLOGIAS DE PONTA

Ao contratar um prestador de serviço nesta área, as empresas têm acesso a tecnologias de ponta e soluções de segurança avançadas. Empresas como a Eurotux procuram diariamente atualizações tecnológicas para oferecer proteção eficaz contra as ameaças mais recentes.

QUERO CONTRATAR UM PARCEIRO PARA CIBERSEGURANÇA, E AGORA?

CONSIDERAÇÕES IMPORTANTES ANTES DE EXTERNALIZAR UM SERVIÇO DE SEGURANÇA:

- **CONFIANÇA E PRIVACIDADE DE DADOS:** a empresa tem práticas adequadas de privacidade e conformidade com regulamentações relevantes para proteger seus dados confidenciais?

- **COMPATIBILIDADE COM A INFRAESTRUTURA EXISTENTE:** os serviços são compatíveis com a sua infraestrutura de TI existente? A integração com sistemas legacy e requisitos específicos é tida em consideração?

- **GESTÃO E RESPONSABILIDADE:** Existe uma clara definição de papéis e responsabilidades para a gestão efetiva da cibersegurança?

Ao apostar num serviço de "Security as a Service", a empresa consegue aceder a competências especializadas e tecnologias avançadas para proteger de forma mais eficaz a sua rede e os seus dados. Serviços como o *Security Operations Center (SOC)* da Eurotux permitem reduzir o investimento ao mesmo tempo que conferem acesso a uma abrangente lista de vantagens. Com diferentes níveis de serviço, o SOC garante acesso a opções de monitorização da rede, suporte, análise e resposta a incidentes, testes à infraestrutura e outros serviços complementares.

- ***ENTRE EM CONTACTO CONNOSCO*** E FIQUE A SABER MAIS SOBRE O NOSSO SERVIÇO SOC.

CASO DE ESTUDO
DIGITALSIGN

EUROTUX DISPONIBILIZA SERVIÇO SECURITY OPERATIONS CENTER NA DIGITALSIGN

A PLATAFORMA SOC ASSEGURA UMA MONITORIZAÇÃO 24 HORAS POR DIA DE EVENTOS DE CIBERSEGURANÇA

A DigitalSign é uma empresa portuguesa, fornecedora de serviços de confiança acreditada na Europa pela eIDAS e no Brasil pela ICP Brasil. A empresa oferece uma vasta gama de serviços, desde certificação digital, plataformas de assinatura, selos de faturas electrónicas, Time Stamp, entre outras.

Com vários anos de experiência no mercado, a DigitalSign disponibiliza certificação digital para responder às mais diferentes necessidades do mercado e oferece soluções personalizadas para as particularidades de cada cliente na Europa e no Brasil. Neste momento, tem cerca de 200 colaboradores diretos, a que se somam 800 indiretos.

DESAFIO

A DigitalSign coloca a segurança na vanguarda da sua proposta de valor. No momento atual, em que os ciberataques estão a tornar-se cada vez mais comuns e mais destrutivos, é mais importante do que nunca tomar medidas para proteger os dados.

A empresa identificou a necessidade de reforçar as medidas de segurança, tais como a certificação ISO27001 e a conformidade eIDAS. A importância de proporcionar aos seus clientes a tranquilidade de que os seus dados estão seguros é um desafio a que Digitalsign se propõe dedicar e responder assertivamente.

Ao aplicar de forma efetiva estas medidas, é possível demonstrar o compromisso com a segurança e a dedicação em fornecer aos clientes o melhor serviço possível.

Não há dúvida de que as ciberameaças aumentaram nos últimos anos. Este cenário, por sua vez, levou à necessidade de uma abordagem mais madura da monitorização da segurança tanto na vertente infraestrutural como na vertente aplicacional. A monitorização ad hoc da segurança simplesmente já não era suficiente para a DigitalSign. Em vez disso, a empresa procurava um sistema de monitorização contínua de sistemas, de forma a aumentar a eficácia e a rapidez no que respeita a identificar riscos potenciais e tomar medidas para os mitigar.

SOLUÇÃO

Dada a natureza do seu negócio, a Digitalsign assume-se como uma empresa que, na essência, vende confiança aos seus clientes. Nesse sentido, as decisões estratégicas são tomadas com esse foco e aplicam-se aos serviços, às equipas internas e à qualidade que coloca nos serviços e produtos. Só é possível assegurar que a confiança não é defraudada se estes (e outros) fatores estiverem assegurados.

Em colaboração com a Eurotux, foi colocado em funcionamento um serviço SOC – Security Operations Center analisando eventos de cibersegurança 24 horas por dia.

Ao recorrer ao SOC, a DigitalSign pretendia responder de forma rápida e eficaz a potenciais ameaças, assim como investigar e resolver incidentes, baseando esta abordagem numa correlação de dados essencial para reforçar a identificação de potenciais problemas e a sua rápida resolução.

RESULTADO

O serviço SOC assumiu-se para a DigitalSign como uma camada valiosa de proteção dos dados e sistemas dos clientes. Tornou-se ainda na garantia de medidas e políticas de segurança ao mais alto nível. Com a colaboração da Eurotux, a Digitalsign consegue neste momento monitorizar as tendências de cibersegurança e fazer alterações ao serviço conforme necessário para assegurar que os seus clientes estão sempre protegidos.

Para a DigitalSign, a implementação dos módulos de SOC permitiu a eliminação de uma estratégia de análise isolada de eventos de cibersegurança *"numa abordagem que carecia de contexto"*, como diz Fernando Moreira, CEO da DigitalSign.

Depois da ativação do serviço SOC, tornou-se possível criar correlações de eventos dentro da infraestrutura da DigitalSign, uma abordagem diferente *"porque permite tirar conclusões que se traduzem na real identificação de riscos"*. Desta forma, é possível, por exemplo, relacionar acessos e eventos. O CEO da empresa de certificação digital explica: *"o utilizador X acedeu a um serviço da DigitalSign a partir de uma rede portuguesa (o que é habitual) e poucos minutos depois acedeu a outro serviço DigitalSign a partir de uma rede espanhola (o que também pode ser perfeitamente natural). Se analisados isoladamente, são comportamentos teoricamente legítimos; mas conjugados demonstram uma elevada probabilidade de uma tentativa de intrusão"*.

No que respeita ao negócio, a parceria com a Eurotux, nomeadamente, a implementação do serviço SOC, permitiu robustecer a qualidade da oferta do serviço da DigitalSign, reforçar a fiabilidade no que respeita a cibersegurança, dotando a empresa de uma visão transversal *"que permite tomar as decisões certas no momento certo"*.

"Trabalhamos com a Eurotux há vários anos, e, durante todo esse tempo, sempre se revelou um excelente parceiro. A empresa é célere a responder às necessidades e beneficia de um conjunto de conhecimentos e experiência que tem sido inestimável para a DigitalSign."

Fernando Moreira, CEO DigitalSign.