00 dias 14 horas 15 min. 28 seg.

10 de Outubro - IT Security Conference - Lisboa - Conheça o programa aqui

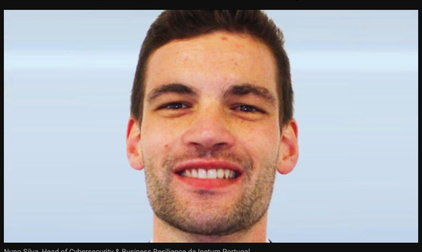
claranet Make modern happen 360 Security Audit

OPINION

A Revolução Silenciosa: cibersegurança como um escudo invisível das empresas contra as ameaças digitais

Ao longo dos últimos anos, testemunhámos uma revolução silenciosa na forma como interagimos com a tecnologia. Desde a proliferação de smartphones até à ascensão das redes sociais, muitas das mudanças que moldam a nossa vida quotidiana ocorreram, gradualmente, sem grande alarido e com naturalidade

Por Nuno Silva, Head of Cybersecurity & Business Resilience da Inetum Portugal . 09/10/2024



Nuno Silva, Head of Cybersecurity & Business Resilience da Inetum Portugal

Mas o potencial da tecnologia ultrapassa a consciência da grande maioria dos utilizadores. Enquanto, por um lado, somos capazes de dar conta das novas funcionalidades cada vez que atualizamos uma aplicação, muitas das mudanças que acontecem no universo da tecnologia são silenciosas e passam despercebidas ao utilizador comum.

É o caso dos avanços ao nível da cibersegurança – que, mais do que uma prioridade, é uma necessidade crescente e essencial para todos os utilizadores, sejam estes utilizadores individuais ou empresas. Vivemos numa época pautada pela evolução constante das ameaças digitais e uma crescente complexidade dos riscos que lhes estão associados.

À medida que as ameaças cibernéticas se tornam cada vez mais sofisticadas, torna-se imperativa a necessidade de implementar medidas de segurança robustas e adaptadas ao contexto de cada organização. Além disso, existem obrigações regulatórias crescentes que exigem a implementação de processos, procedimentos e de tecnologia que aumente a resiliência das organizações e acelere a capacidade de resposta a incidente de cibersegurança. Exemplo disso é a recente Diretiva NIS2, uma legislação europeia que está a revolucionar a forma como as empresas abordam a cibersegurança nas suas operações.

Enquanto a maioria de nós está ocupada com as inovações tecnológicas mais práticas e percetíveis, como a inteligência artificial e 'Internet das Coisas', a implementação das diretivas como a NIS2 está a acontecer discretamente, mas com um impacto significativo. Esta nova Diretiva vem preencher uma lacuna essencial na abordagem da União Europeia à cibersegurança no universo corporativo. Ao contrário da anterior NIS1 que se limitava um conjunto muito restrito de sectores esta norma adota uma abordagem abrangente e holística, reconhecendo que a cibersegurança se torna um fator imperativo para um conjunto alargado de sectores incluindo, empresas de média dimensão com um volume de faturação superior a 10M€.

Podemos criar o paralelismo com a necessidade de um bom sistema de alarmes numa casa onde, independentemente do tamanho, a segurança é sempre uma prioridade. Para uma grande mansão, com grandes jardins e inúmeras janelas, é recomendável câmaras de vigilância, talvez alguns vigilantes a patrulhar a propriedade e alarmes sofisticados. No entanto, até um apartamento, embora mais modesto e menos chamativo, também precisa de trancas nas portas para que os seus inquilinos possam dormir descansados.

Da mesma forma, seja uma organização multinacional, com enormes recursos financeiros, operações sensíveis e alto risco de ataques cibernéticos, ou uma PME, com um negócio mais singelo, a necessidade de cibersegurança é inegável.

Neste contexto, são também inegáveis os desafios que as empresas enfrentam para adaptar ou implementar soluções robustas e efetivas, proporcionais ao seu nível de risco, mantendo em simultâneo esta revolução impercetível aos olhares mais destreinados. A adaptação a esta nova diretiva irá obrigar muitas empresas a um esforço na implementação de novos sistemas de TI e processos operacionais que exigem uma colaboração entre diferentes áreas da empresa, uma cultura de gestão da mudança forte para que esta transformação ocorra da forma mais ágil e suave possível. Se for bem realizada, irá traduzir-se num processo invisível e silencioso dentro da organização, munido das ferramentas certas para endereçar os novos desafios e requisitos regulamentares de cibersegurança.

À medida que as empresas se adaptam a esta nova realidade digital de proteção, é crucial compreender que a cibersegurança não se trata apenas de uma tendência passageira, mas sim de uma necessidade contínua e crescente que moldará o futuro da interação de todos com a tecnologia. Mas manter-se-á esta uma revolução silenciosa? Ou novas diretivas como esta serão o holofote para evidenciar falhas estruturais ao nível de cibersegurança corporativa?

Nuno Silva | Cibersegurança

RECOMENDADO PELOS LEITORES

OPINION
Como lidar com dispositivos não geridos nos novos ambientes Zero Trust

OPINION
Até dia 10

OPINION
A ascensão das "redes sociais" de crime informático

factis 4me Mais

REVISTA DIGITAL
IT SECURITY Nº20 Outubro 2024
DOWNLOAD AQUI!
IT SECURITY
CONSOLIDAÇÃO DA CIBERSEGURANÇA
EDIÇÕES ANTERIORES

NEWSLETTER

Receba todas as novidades na sua caixa de correio!

O seu email... Subscrever

360 Security Audit claranet

+ VISITADAS

25/09/2024
PODCAST
Pentest & DevSecOps e o enquadramento com a DORA, NIS2 e IA Generativa em destaque no mais recente episódio do IT Security Watch

24/09/2024
ITS CONF
Inscrições esgotadas para a IT Security Conference 2024, mas pode assistir gratuitamente via Zoom

30/09/2024
S.LABS
Os desafios do Regulamento DORA e a Diretiva NIS2

01/10/2024
FLASH SECURITY
IT Security tem novo podcast durante o Mês Europeu da Cibersegurança

24/09/2024
NEWS
Microsoft recebe certificação do Gabinete Nacional de Segurança

+ NOTÍCIAS

01/10/2024
OPINION
A ascensão das "redes sociais" de crime informático

30/09/2024
OPINION
Até dia 10

20/09/2024
OPINION
Como lidar com dispositivos não geridos nos novos ambientes Zero Trust

30/08/2024
OPINION
Do Shadow IT ao Shadow AI: o perigo do uso não autorizado de IA nas empresas

20/08/2024
OPINION
Regras de Ouro de Data Loss Prevention

It Insight Security
Seguir Página 110 seguidores

It Insight Security
Há 41 minutos
José Luís Silva, da Timestamp SGS, explica neste episódio em que medida é que o XDR e o SIEM diferem
ITSECURITY.PT
Em que difere o XDR do SIEM em des...
Gosto Comentar Partilhar

It Insight Security
há 5 horas
A Google lançou correções para 26 vulnerabilidades de alta severidade como parte da atualização de segurança de outubro de 2024

O nosso website usa cookies para garantir uma melhor experiência de utilização. ACEITAR