METALSHOE
FABLAB NETWORK

10

Referencial Técnico

CIBER-SEGURANÇA

catim
centro de apoio tecnológico à indústria metalomecânica

ctcp centro tecnológico do calçado de portugal

NORTE 2020
PROGRAMA OPERACIONAL REGIONAL DO NORTE
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

METALSHOE
FABLAB NETWORK

10

www.metalshoefablab.pt

Referencial Técnico

CIBER-SEGURANÇA

Ficha técnica

Título
10 Referencial Técnico - Cibersegurança

Coordenação
Cristina Marques e Vânia Pacheco

Projecto gráfico e paginação
SALTO ALTO ctcp criativo

Textos
Cristiano Figueiredo
Gonçalo Costa
Luis Rocha
Maria Fernandes

Com o apoio de
AIDUST, Consultadoria e Apoio à Indústria S.A

Versão 01

Este referencial foi desenvolvido no âmbito
do projeto Metalshoe Fablab Network
Operação Nº NORTE-02-0853-FEDER-037621

catim
centro de apoio tecnológico à indústria metalomecânica

ctcp centro tecnológico do calçado de portugal

NORTE 2020
PROGRAMA OPERACIONAL REGIONAL DO NORTE

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

ÍNDICE

INTRODUÇÃO

O presente referencial está integrado num conjunto de documentos técnicos a disponibilizar no âmbito do projeto MetalShoe FabLab Network, apoiado pelo NORTE2020 e promovido pelo Centro Tecnológico do Calçado de Portugal (CTCP) e pelo Centro de Apoio Tecnológico à Indústria Metalomecânica (CATIM). Procura-se, assim, apoiar a indústria dos setores do calçado, metalúrgico e metalomecânico no uso de tecnologias avançadas e no desenvolvimento de produtos inovadores recorrendo à utilização de determinadas tecnologias, algumas delas emergentes, outras já conhecidas e integradas pelo tecido industrial, mas ainda sem uso generalizado por estes setores.

No passado, os sistemas de produção eram fechados, não estavam expostos a redes externas e por isso, inerentemente, seguros relativamente a acessos remotos. O seu controlo era apenas físico, com as normais limitações no tempo de resposta e acesso a informações.

Atualmente, com a desenvolvimento da indústria 4.0, as organizações preocupam-se cada vez mais em automatizar os processos, na melhoria contínua, com a partilha de dados, com sistemas interligados, máquinas equipadas com dispositivos inteligentes (sensores, atuadores, câmaras, etc.), que são conectados via redes sem fios (comunicação wireless WiFi, Bluetooth, Wimax, LoraWan, redes móvel 2G, 3G,4G e 5G) [1] com outras máquinas ou com softwares de gestão. Isto resulta na criação de uma grande quantidade de dados, frequentemente guardados na "nuvem" e em constante circulação. Assim, tornaram-se atrativos os ataques cibernéticos na tentativa de roubos de informação da organização, de servidores localizados "dentro de portas", o que começou a preocupar as organizações. Criam-se, desta forma, as ferramentas de e mecanismos de defesa contra estes ataques, aqui englobados no conceito de cibersegurança, para a proteção de todos os dados da organização aos ataques cibernéticos [2].

Este referencial foca-se na cibersegurança industrial, no que esta representa dentro duma organização industrial, que ameaças existem, os diferentes tipos de cibersegurança e, também que medidas tomar de cibersegurança numa organização. Sem tentar ser demasiado extensivo e profundo acerca desta temática, este referencial serve, assim, como ponto de partida para notar às organizações a necessidade de darem mais atenção a este tema.

CIBERSEGURANÇA, HACKERS E CIBER-CRIMINOSOS

Cibersegurança, tal como implícito no nome, é a segurança de sistemas ciber, isto é, dos sistemas digitais. Cibersegurança é uma das mais importantes componentes da indústria 4.0, interagindo com todas as outras componentes, como o IOT (Internet Of Things – Internet das Coisas), a automação, a robótica, ou o big data. Frequentemente, todas estas componentes implicam a gestão de e partilha de dados e ligação à nuvem, necessitando de proteção.

A hipótese de ataques cibernéticos deve ser considerada no instante projeto do Sistema de Controlo Industrial (SCI). No entanto, a cibersegurança nas pequenas e médias empresas (PMEs) ainda não é vista como um requisito obrigatório de implementação na organização, mas sim como um extra que um dia poderão vir a implementar, com consequências que podem ser nefastas devidas à sua tardia aplicação [3].

Existem várias estratégias diferentes para combater os ataques aos SCI. Estas têm diferentes custos económicos, graus de eficiência e de complexidade distintos, apresentando-se a lista de algumas delas [4]:

- Software antivírus;
- Backups automáticos fora do local;
- Planos de recuperação de desastres;
- Zonas desmilitarizadas;
- Encriptação de dados;
- Firewalls industriais;
- Sistemas de deteção de intrusões;
- Autenticação multifator;
- Dispositivos de monitorização da rede;
- Segmentação de rede;
- Gestão e procedimentos de senhas;
- Gestão de patchs (software de computador criado para atualizar ou corrigir um software de forma a melhorá-lo);
- Configuração das portas;
- Redundância dos sistemas;
- Software de gestão remota;
- Gestão de incidentes de segurança e eventos;
- Díodos unidirecionais de dados;
- Redes privadas virtuais;
- Software de digitalização de vulnerabilidades;
- Gestão dos pontos de acesso sem fios.

Existem dois tipos de "ciberatacantes", o hacker e o cibercriminoso, por vezes confundidos como sendo o mesmo, mas com diferenças entre os dois.

Hacker é um indivíduo, normalmente, especialista em programação de computadores, que usa as suas capacidades para conseguir entrar em sistemas digitais, redes e dispositivos que não lhe pertencem, tanto com propósitos bem-intencionados como mal-intencionados. Por vezes, os hackers trabalham em conjunto com profissionais de cibersegurança para o desenvolvimento de melhores estratégias de cibersegurança. Os profissionais de cibersegurança identificam os riscos de segurança, e os hackers ajudam a perceber onde existem lacunas no sistema por onde outros hackers poderiam fazer um ataque.

De acordo com o *The Sans Institute* [5], existe 3 categorias de hackers:

White Hat: trabalha dentro das leis da ética do hacker (não fazer dano), ou como perito de segurança.

Black Hat: estes são hackers, geralmente, motivados pelo poder, raiva ou ódio. São caracterizados por não terem quaisquer problemas em destruir os dados das redes em que obtêm acesso, e não têm qualquer propósito de bondade nas suas ações.

Gray Hat: este termo foi criado por L0pht, um dos melhores grupos de hackers localizados em Boston. Normalmente, este tipo de hackers já pertenceu ao grupo "Black Hat", tendo-se tornado posteriormente consultores de segurança.

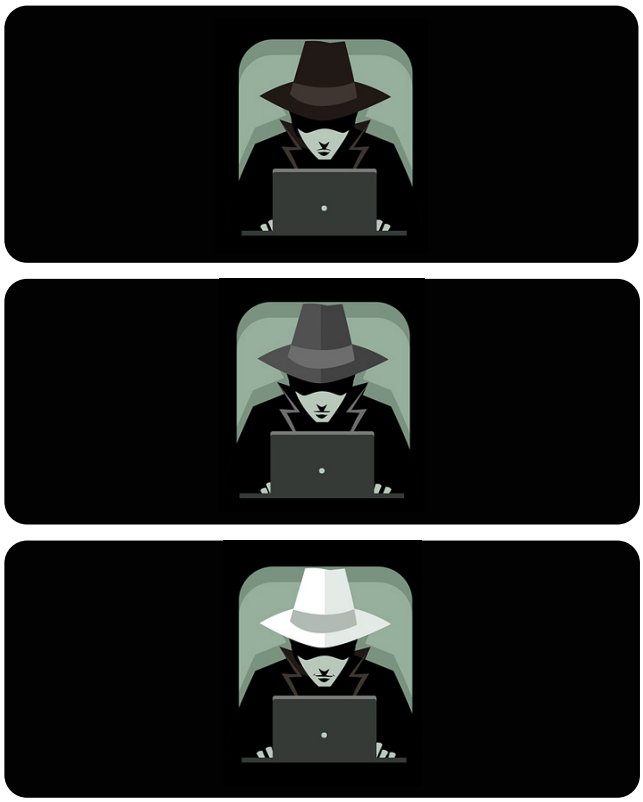
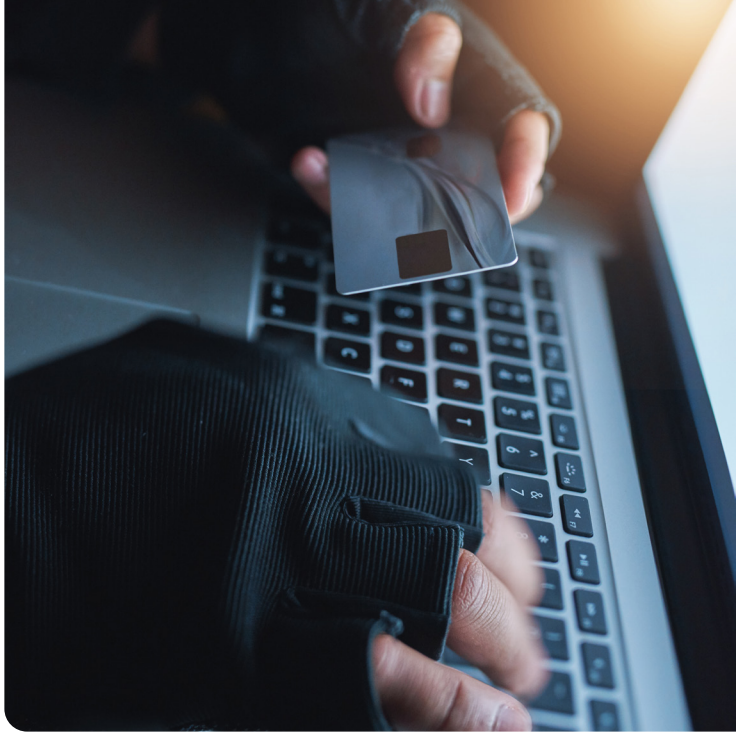


Figura 1 Imagem ilustrativa do Black Hat, Gray Hat e White Hat[6].

A definição de cibercriminoso pode ser simplificada como um individuo que utiliza um computador, ou outra tecnologia digital como por exemplo a internet, para fazer alguma atividade ilegal. Estes criminosos, podem atuar de forma solitária, roubando informações para a obtenção de ganhos financeiros, ou atuar de uma forma mais organizada em grupo, utilizando meios como a internet, para infringir a lei em atividade como comprar e vender mercadorias ilegais, roubar informações, espiar, etc.[7]



AMEAÇAS E ESTRATÉGIAS PARA A CIBERSEGURANÇA

Tipos de ameaças cibernéticas comuns

Existem vários tipos de ameaças cibernéticas, de acordo com a forma e os métodos usados e o grupo-alvo atacado, que se detalha de seguida:

Malware

É, de uma forma simples, um tipo de software projetado para obter acesso não autorizado ou causar danos a um computador [8]. Existem 6 tipos diferentes de malware:

- **Vírus**: programa autorreplicante que se anexa a um arquivo/ficheiro limpo e se espalha por um sistema de computador, infetando ficheiros com código nocivo [9].
- **Trojans**: tipo de malware disfarçado de software legítimo. Os cibercriminosos induzem os utilizadores a executarem "cavalos de Troia" nos seus computadores, resultando em danos ou roubo de dados [9].
- **Spyware**: software que regista de forma secreta as interações do utilizador com o computador, como introdução de passwords, páginas visitadas, dados de cartões de crédito, entre outras, para que estas informações possam ser usadas pelos cibercriminosos [9].
- **Adware**: software de publicidade que pode ser usado para espalhar malware [9].
- **Botnets**. redes de computadores infetadas por um ou mais bots, softwares autónomos, que os cibercriminosos usam para realizar tarefas online sem a permissão do utilizador [9].
- **Ransomware**: tipo de software enganador, normalmente projetado para extorquir dinheiro, bloqueando o acesso a arquivos ou ao sistema do computador até que o resgate seja pago. Pagar o resgate não garante que os arquivos sejam recuperados ou o sistema restaurado [8].

Phishing

Prática de enviar e-mails falsos idênticos a e-mails de fontes fidedignas. O objetivo passa por roubar dados confidenciais, como números de cartão de crédito e informações de login. É o tipo mais comum de ataque cibernético [8].

Engenharia social

É uma tática que os atacantes usam para induzir a revelação de informações confidenciais. Habitualmente, solicitam um pagamento monetário, dados de login, ou outros dados confidenciais. A engenharia social aparece, muitas vezes, com outras táticas levando os utilizadores mais incautos a clicar em links perniciosos, fazer download de malware ou confiar em fontes enganadoras [8].

Ameaças internas

Dentro das organizações, funcionários atuais ou antigos, parceiros de negócios, contratados externos ou qualquer pessoa que tenha tido acesso aos sistemas ou redes da organização no passado podem ser considerados uma ameaça interna se abusarem das suas permissões de acesso e estas não lhes forem retiradas devidamente [10].

Distributed Denial of Service (DDoS)

Um ataque DDoS tenta bloquear um servidor, site ou rede, sobrecarregando-o com tráfego, geralmente de vários sistemas coordenados. Os ataques DDoS sobrecarregam as redes corporativas por meio do protocolo simples de gestão de rede (SNMP), usado para routers, impressoras, switches (principal funcionalidade a interligação de equipamentos (estações de trabalho, servidores, etc.) de uma rede[11]) e servidores [10].

Ameaças Persistentes Avançadas (APTs)

Nesta situação, um intruso ou grupo de intrusos infiltra-se num sistema e permanece sem ser detetado por um longo período. O intruso deixa as redes e sistemas intactos para que possa espiar a atividade comercial e roubar dados confidenciais, assim evitando o ativar das medidas defensivas [10].

Ataques Man In The Middle (MITM)

É um ataque de espionagem, em que um cibercriminoso intercepta e retransmite mensagens entre duas partes para roubar dados. Por exemplo, numa rede Wi-Fi insegura, um invasor pode intercetar dados transmitidos entre o dispositivo do convidado e a rede [10].

Tipos e princípios de cibersegurança

Para proteger dos possíveis ciberataques, existem algumas estratégias de segurança como as que se listam:

Segurança de aplicações: Estratégia geral que foca em manter o software e os dispositivos livres de ameaças. Uma simples aplicação, ou programa, comprometida pode fornecer acesso a dados que foi projetada para proteger. A segurança bem-sucedida começa, na fase do projeto, no seu design, antes de um programa ou dispositivo ser sequer implementado ou programado [13].

Segurança de rede: Plano para proteger uma rede de computadores, dispositivos, contra ameaças, sejam elas de hackers direcionados ou malware oportunista. Este planeamento de segurança visa garantir que o acesso aos dados circulantes entre os diferentes dispositivos da empresa seja feito apenas por quem tiver autorização [13].

Segurança na nuvem: Medidas contra ameaças externas que protegem os dados que se encontram armazenados na nuvem mas, também, os dados em movimento entre os utilizadores e os locais de armazenamento [13].

Segurança de informação: Relacionado com as anteriores, medidas gerais que protegem a integridade e a privacidade dos dados, tanto no armazenamento quanto no trânsito [9], isto é, quando os dados se encontram a circular entre dispositivos [10].

Segurança de infraestrutura crítica: Conjunto de práticas usadas para proteger sistemas de computadores, redes e outros ativos dos quais a comunidade depende de forma crucial para segurança nacional, saúde económica e/ou segurança pública.

No caso particular de empresas, estas possuem também sistemas incluídos na sua infraestrutura crítica que são essenciais para o seu funcionamento, como sistemas de controle industrial, sistemas de controle de supervisão e aquisição de dados (SCADA), que são usados para automatizar processos industriais. Ataques ao SCADA e a outros sistemas de controle industrial são preocupantes.

Eles têm a capacidade de prejudicar seriamente a infraestrutura crítica, incluindo o transporte, fornecimento de petróleo e gás, redes elétricas, distribuição de água e recolha de águas residuais. É por isso importante serem implementadas estratégias de defesa contra ataques a estes sistemas. [13].

Segurança móvel: Os dispositivos móveis, como telemóveis ou tablets, são cada vez mais centrais no dia a dia, sendo uma ferramenta essencial de trabalho, onde está armazenada uma quantidade significativa e importante de informação, desde dados pessoais a informações comerciais e industriais. Daqui se percebe, a relevância que as práticas de segurança móvel são cruciais [13].

Segurança IoT: Dispositivos e sistemas IOT, ligados em rede, muitas vezes sem fios, são frequentemente concebidos com pouca segurança nos seus protocolos de partilha de dados [15]. Estes são responsáveis pelo processamento de dados de produção na indústria e a nível industrial, sendo frequentemente objeto de ameaças, como MITM, SQLI e DDoS [13]. Deve ser dada particular atenção a estes dispositivos quando implementados nas redes.

Educação do utilizador final: O elemento mais imprevisível da cibersegurança é o fator humano, isto é, os utilizadores. Qualquer pessoa pode acidentalmente introduzir um vírus, ou outra qualquer ameaça, num sistema seguro caso as melhores práticas de segurança não sejam seguidas [10]. Para além das medidas técnicas de proteção, como o controlo de acessos, permissões, capacidade de executar software, ou mesmo restrição física na utilização de equipamentos, é essencial educar os utilizadores acerca das ameaças possíveis e das suas consequências.

Medidas de cibersegurança

A segurança das organizações e a proteção das informações destas, implica a adoção e a boa implementação de medidas de cibersegurança. Isto é crucial para o bom funcionamento das entidades, da relação com os parceiros e tem impacto significativo no negócio e o seu crescimento.

Para a definição de uma estratégia de cibersegurança é importante a colaboração com um parceiro com capacidade tecnológica para fazer uma análise cuidada dos requisitos, estabeleça um método de trabalho e um plano de defesa contra ameaças. Apresenta-se, de uma forma genérica, uma lista de medidas a seguir para a implementação dos requisitos de cibersegurança numa organização [16][17]:

Identificar ativos

O primeiro passo para proteger uma organização contra ameaças cibernéticas é identificar quais os ativos da organização que podem ser alvo de interesse por outros. Torna-se, ainda, mais importante identificar os ativos, dispositivos ou dados, informações de valor para os cibercriminosos, sem os quais a organização teria dificuldade em continuar a trabalhar e dos quais depende a sua rentabilidade.

Proteger ativos

Identificados os ativos, torna-se necessário desenvolver a estratégia da sua proteção. Os intervenientes, principalmente funcionários das empresas, são fundamentais para este processo da segurança cibernética, interiorizando e reconhecendo os riscos a que estão expostos, e os riscos para o negócio. À medida que a organização cresce e implementa no seu fluxo de trabalho novas tecnologias e/ou funções, as estratégias de segurança devem ser repensadas e adaptadas, ou mesmo reforçadas.

Detetar ataque

Identificar e proteger os ativos, não impede de sofrerem tentativas de ataques. Deve haver uma definição e implementação de medidas para que, de forma atempada, se detetem estes eventos. Quanto mais rápido se detetar um ataque, mais rápido se poderá eliminar o perigo e a ameaça de roubo de informações sensíveis ou de perturbações na produção.

Responder aos ataques

No seguimento da deteção de um ataque, é importante ter um plano para responder a este, antes de ter reais consequências e para uma resposta bem-sucedida. É importante haver um plano que os responsáveis conheçam e implementem de forma imediata. Como primeira resposta, caso esteja a acontecer algum ataque, a primeira coisa a fazer poderá ser desconetar o dispositivo/sistema da rede ou mesmo da energia [18].

Recuperar

Caso um ataque seja bem-sucedido, ou tenha tido qualquer impacto, é necessário aplicarem-se estratégias de recuperação que devem ter sido previamente preparadas. O objetivo da recuperação é ultrapassar as consequências causadas pelo ataque cibernético restaurando completamente os sistemas e operação normal da instituição. Durante a etapa de recuperação, deve também identificar-se como foi feito o ataque e qual o processo que permitiu ultrapassar as barreiras de segurança, informando assim as estratégias futuras, permitindo uma correção das medidas de segurança e a prevenção de eventos futuros.

Certificação de cibersegurança nacional

O caminho para a certificação como processo, permite avaliar a situação da segurança dos sistemas, sendo um instrumento importante no autoconhecimento e nas medidas que podem e devem vir a ser tomadas para se tornarem as instituições mais seguras.

A certificação de cibersegurança é um processo que verifica se uma entidade, serviço, processo ou produto cumpre com os requisitos de cibersegurança em relação às suas componentes de Tecnologias de Informação e Comunicação (TIC).

Isso é feito através da aplicação de uma metodologia de avaliação reconhecida pelas entidades competentes como idónea para esse fim. As auditorias e demais atividades de avaliação, como a condução de testes em laboratório e a análise documental, são conduzidas sob a orientação de uma entidade certificadora independente, o organismo de certificação, acreditado por um organismo nacional de acreditação.

O organismo de certificação emite o certificado quando se verifica o cumprimento dos requisitos, frequentemente uma norma publicada por um organismo de normalização que define um conjunto de critérios e condições técnicas, sob as regras definidas no esquema de certificação [19].

Benefícios da certificação

A certificação de cibersegurança é uma forma de elevar o nível de segurança de uma entidade. Isso é feito através da adoção de práticas estruturadas e permanentes de cibersegurança que reduzem os riscos e aumentam a proteção contra incidentes e ciberataques.

A certificação promove a confiança dos clientes, utilizadores e outras partes interessadas da entidade para uma utilização e relacionamento seguros com esta. A obtenção e divulgação da certificação da cibersegurança por uma entidade permite-lhe a demonstração de vantagem competitiva sobre a concorrência, assim como o aumento da reputação e melhoria geral da sua imagem [19].

Notícias de casos de ataques cibernéticos e cibersegurança

Não sendo uma situação nova, os ataques cibernéticos têm sido noticiados de uma forma consistente nos tempos recentes. A necessidade de ter uma estratégia para a cibersegurança em cada organização é cada vez mais importante. A economia é crescentemente baseada em informações que, estando em formato de dados digitais, necessitam de particular cuidado com a sua preservação. Apresentam-se à frente recortes e citações de algumas situações noticiadas na comunicação social durante os últimos meses.

"No que respeita à área de cibersegurança, "e até pela situação concreta da guerra na Ucrânia, estamos neste momento com um diagnóstico que claramente mostra" que, "por exemplo, janeiro deste ano foi o mês com maior incidentes registados, da ordem de quase 300 incidentes registados pelo nosso CERT ['Computer Emergency Response Team'], ou seja, a equipa que responde precisamente a estas situações de emergência", disse o secretário de Estado aos deputados." [20].

"Os dados pessoais dos clientes da TAP divulgados pelo grupo de cibercriminosos Ragnar Locker, que atacou a companhia aérea em agosto, vão do nome, morada, email, data de nascimento até data de registo e número de passageiro."
"Embora os ciberataques constituam uma ameaça constante para muitas empresas, a TAP tomou imediatamente medidas para a contenção e resolução do incidente, de forma a proteger todos os dados detidos ou geridos", salientou." [21].


Cibersegurança

Ameaças online detetadas aumentaram 42% entre janeiro e abril

IN/Agências
08 Novembro 2022 às 14:48

COMENTAR

TÓPICOS
Nacional

Incidentes aumentaram 42% entre janeiro e abril
Foto: DR

O secretário de Estado da Digitalização e da Modernização Administrativa afirmou que, entre janeiro e abril deste ano, os incidentes registados aumentaram 42% em termos homólogos, sublinhando a importância de boas práticas de cibersegurança.

Mário Campolargo falava no âmbito da discussão do Orçamento do Estado para 2023 (OE2023), na comissão parlamentar conjunta de orçamento e Finanças, de Economia, Obras Públicas, Planeamento e Habitação e de Administração Pública, Ordenamento do Território e Poder Local.

Figura 2 Captura de ecrã do site: JN de notícia de 8 novembro 2022 [20].


MENU 11

Diário de Notícias

INÍCIO / SOCIEDADE

Hackers publicam dados de 1,5 milhões de clientes da TAP

Piratas informáticos dizem ter acesso remoto a sistemas da transportadora aérea, avança o Expresso. TAP diz não ter indicação de que piratas tenham tido acesso a dados de pagamento

DN
20 Setembro 2022 — 08:47

TÓPICOS
ciberataques
Sociedade
TAP

O grupo de hackers Ragnar Locker cumpriu a a ameaça que vinha a fazer e publicou esta segunda-feira na Dark Web 581 gigabytes (GB) de dados que diz serem referentes a 1,5 milhões de clientes da TAP e garante que continua a ter acesso aos sistemas informáticos da transportadora, avança o Expresso.

Figura 3 Captura de ecrã do site: Diário de Notícias de notícia de 21 de setembro 2022 [21].

"A média semanal de ciberataques a organizações portuguesas aumentou 81% em 2021, face a 2020, de acordo com os dados mais recentes da empresa de cibersegurança Check Point. Já este ano, Vodafone, Sonae e Impresa (dona do Expresso) foram algumas das empresas alvo de intrusões por parte de organizações criminosas e a Check Point dá conta de uma subida de 42% no primeiro semestre de 2022 nas investidas digitais ilegais a nível global.

Em todo o mundo, os ciberataques custaram mais de €5 mil milhões e, segundo a empresa de análise Cybersecurity Ventures, estima-se que o rombo económico suba 15% anualmente, até ultrapassar os €8 mil milhões em 2025. "Estamos quase num ambiente de guerra", resume o diretor de Sistemas de Informação da Asseco, Miguel Rodrigues. A instabilidade global acelerou as tendências e "a pandemia intensificou a conflitualidade no ciberespaço, na medida em que a densidade digital foi reforçada, criando uma maior superfície de ataque." [22].

"O mercado português de cibersegurança vale €165 milhões, de acordo com o mais recente relatório do Observatório de Cibersegurança do Centro Nacional de Cibersegurança, o que coloca o país na cauda da Europa. Na opinião de Rui Duro, country manager da Check Point, "ainda não foi feito o suficiente" em Portugal, com a certeza de que "a criação de hábitos de higiene cibernética requer tempo e investimento". Porém, importa realçar que "começamos a ver uma aposta na formação contínua dos colaboradores". Acrescenta Lino Santos que, "com a transição das equipas para formatos laborais mais flexíveis, como os regimes híbrido e remoto, manifestou-se uma maior preocupação por parte das empresas" neste campo.

O que é fulcral quando o "Threat Landscape Report", da S21Sec, mostra que Portugal ocupou o 37º lugar no ranking mundial de ciberataques no primeiro semestre de 2022."[22].


Expresso

Países com melhor índice de cibersegurança

2020

POSIÇÃO	PAÍS
1º	EUA
2º	Reino Unido
2º	Arábia Saudita
3º	Estónia
4º	Coreia
4º	Singapura
4º	Espanha
5º	Rússia
5º	EAU
5º	Malásia
6º	Lituânia
7º	Japão
8º	Canadá
9º	França
10º	Índia
11º	Turquia
12º	Áustria
13º	Luxemburgo
13º	Alemanha
14º	PORTUGAL
15º	Letónia

Fonte: ONU • Criado com Datawrapper

Figura 4 Captura de ecrã do site: Expresso de notícia de 18 novembro 2022 [22].

"O mais surpreendente, segundo revelou esta quarta-feira à Insider Dave Tremper, do Departamento de Defesa dos EUA, foi a velocidade no bloqueio ao ciberataque. Para o responsável do Pentágono, os militares norte-americanos não teriam conseguido travar o ataque tão rápido como a equipa da Starlink."

"A 24 de março, Elon Musk, proprietário da empresa de internet através da SpaceX, tinha afirmado que, até àquela data, a Starlink tinha "resistido a todas as tentativas de ataque e interferência."

Figura 5 Captura de ecrã do site: Observador de notícia de 22 de abril 2022 [23].

Enquadramento no MetalShoe FabLab

O FabLab que resulta do projeto em apreço tem como missão estimular a criatividade e a inovação, aliadas à digitalização, promover iniciativas intersectoriais e a articulação com as entidades do Sistema Científico e Tecnológico Nacional, por forma a garantir que existe uma linha de pensamento e de ação híbrida, onde o design, a estética e a funcionalidade de produto desempenham papeis de elevada importância.

Dentro do MetalShoe FabLab e dos centros tecnológicos onde este se instala, encontra-se uma equipa capacitada para apoiar a indústria no âmbito da digitalização da gestão e dos processos industriais.

O CTCP possui experiência no desenvolvimento de soluções informáticas para a gestão industrial da área do calçado, podendo ao mesmo tempo servir de interface entre as empresas do calçado e os fornecedores desta tecnologia.

Existe também a capacidade de diagnosticar o grau de cibersegurança das empresas, podendo ser feito um acompanhamento por parte da equipa na definição por parte das empresas dos passos a tomar para a cibersegurança, com análise e discussão das soluções e uma definição do caderno de encargos do processo.

Exemplos de casos de aplicação

A indústria de calçado e marroquinaria é, cada vez mais, digital. A informação que usa aloja-se em servidores próprios ou mesmo na nuvem (cloud). As comunicações com os clientes são em suporte digital, seja por email, seja por plataformas dos ERP ou outras, ou mesmo a mais simples mensagem instantânea.

Há segredos industriais desde o calçado de moda, ao calçado técnico que necessitam de proteção. Desta forma, são variados os exemplos onde a cibersegurança se revela particularmente necessária:

- Design e desenvolvimento do produto interno, nomeadamente estilismo, materiais e tecnologias envolvidas.

- Design de produto para private label ou seja, produção para outras marcas em contratação. É, aqui, crucial proteger os dados do cliente e da sua propriedade intelectual.

- Tecnologia do calçado, principalmente ao nível do calçado técnico, frequentemente envolvendo patentes e segredos industriais essenciais às empresas e desenvolvidos por estas com investigação interna.

- Proteção dos dados pessoais de funcionários, de clientes e de fornecedores, e de informações confidenciais da empresa.

- Proteção contra perturbações de funcionamento da produção, nomeadamente contra possíveis ataques a equipamentos e sistemas.

Mostra-se, assim, a necessidade e o impacto que a segurança cibernética tem no funcionamento das organizações. As implicações são muito mais do que perda de informação ou a divulgação de dados para o exterior, podendo ter forte impacto económico, com consequências que podem colocar em causa a sobrevivência das empresas e demais entidades. Estando a cibersegurança relacionada com tudo o que é digital, é essencial um planeamento desde o primeiro momento, prevendo e prevenindo implicações futuras.

BIBLIOGRAFIA

[1] R. Rudenko, I. M. Pires, P. Oliveira, J. Barroso, and A. Reis, "A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity," Electron., vol. 11, no. 11, 2022, doi: 10.3390/electronics111111742.

[2] N. Pires et al., "é a excelência das pessoas que trabalham connosco que garante o sucesso da nossa empresa " ·," 2019.

[3] A. Valenzano, "Industrial cybersecurity: Improving security through access control policy models," IEEE Ind. Electron. Mag., vol. 8, no. 2, pp. 6–17, 2014, doi: 10.1109/MIE.2014.2311313.

[4] "What kind of guidance is available to help you defend your industrial control system (ICS)?".

[5] C. Sweigart, "Interested in learning more ? In sti tu te , A ut ho ins ll r igh," no. Security 401, pp. 1–39, 2003, [Online]. Available: https://www.giac.org/paper/gsec/3907/introduction-computer--security-incident-response/106281

[6] "Black Hat, Gray Hat, White Hat." https://www.searchenginejournal.com/white-hat-vs-black-hat-vs-gray-hat-seo/365142/

[7] "Allstate." https://www.allstateidentityprotection.com/content-hub/the-difference-between-hackers-cybercriminals-and-identity-thieves

[8] "cisco." https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~types-of-threats (accessed Dec. 21, 2022).CSCITA.2014.6839299.

[9] "kaspersky." https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (accessed Dec. 22, 2022).

[10] "ibm." https://www.ibm.com/topics/cybersecurity (accessed Dec. 20, 2022).

[11] "pplware." https://pplware.sapo.pt/microsoft/windows/redes-como-funciona-um-switch/

[12] "w3schools." https://www.w3schools.com/sql/sql_injection.asp (accessed Dec. 22, 2022).

[13] "geeksforgeeks." https://www.geeksforgeeks.org/cyber-security-types-and-importance/ (accessed Dec. 21, 2022).

[14] "mend." https://www.mend.io/resources/blog/ast-application-security-testing/ (accessed Dec. 23, 2022).

[15] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial internet of things: A software-defined networking approach," Comput. Ind., vol. 104, pp. 47–58, 2019, doi: 10.1016/j.compind.2018.10.004.

[16] "National Cybersecurity Alliance." https://staysafeonline.org/programs/cybersecure-my--business/ (accessed Dec. 27, 2022).

[17] C. N. de Cibersegurança, "cncs," QUADRO Nac. Ref. PARA A CIBERSEGURANÇA, vol. 4, no. 1, pp. 88–100, 2019.

[18] C. Readiness, "Cyber Readiness Tips & Guidelines".

[19] "cncs." https://www.cncs.gov.pt/pt/certificacao/ (accessed Dec. 29, 2022).

[20] "JN." https://www.jn.pt/nacional/ameacas-online-detetadas-aumentaram-42-entre-janeiro-e-abril-15330413.html (accessed Dec. 28, 2022).

[21] "dn." https://www.dn.pt/sociedade/hackers-publicam-dados-de-15-milhoes-de-clientes-da-tap-15179930.html (accessed Dec. 28, 2022).

[22] "Expresso." https://expresso.pt/iniciativase-produtos/projetos-expresso/2022-11-18-Cibercrime-dispara-e-ameaca-instituicoes-576d3b99 (accessed Dec. 28, 2022).

[23] "Observador." https://observador.pt/2022/04/22/pentagono-surpreendido-com-velocidade-com-que-starlink-travou-ciberataque-russo/

METALSHOE

FABLAB NETWORK

catim
centro de apoio tecnológico à indústria metalomecânica

ctcp centro tecnológico do calçado de portugal

NORTE 2020
PROGRAMA OPERACIONAL REGIONAL DO NORTE

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional