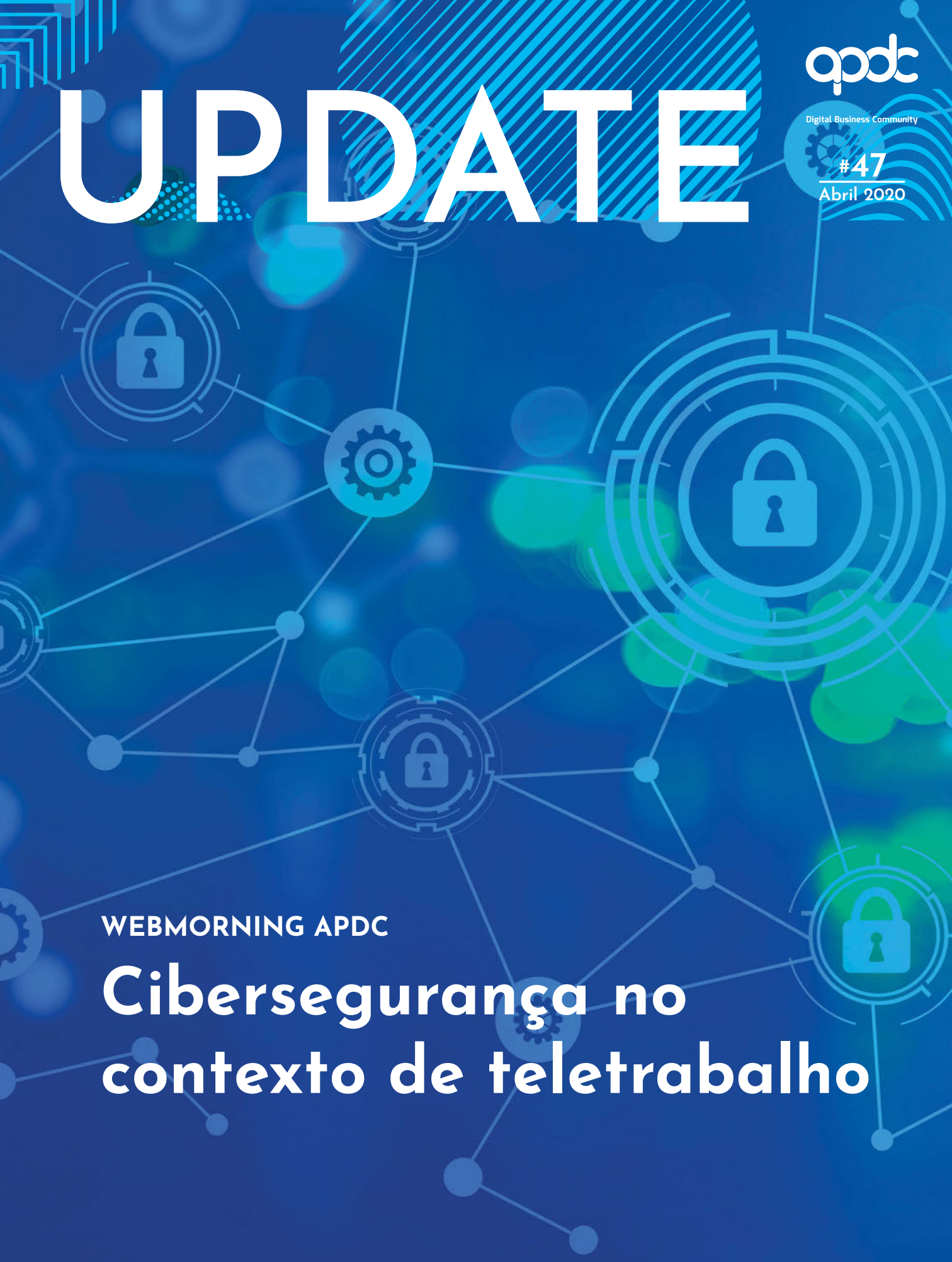
UPDATE

apdc
Digital Business Community
#47
Abril 2020



WEBMORNING APDC

Cibersegurança no contexto de teletrabalho

Como proteger um futuro cada vez mais digital?

A pandemia trouxe consigo o isolamento social, com a consequente adoção massiva do trabalho remoto. Uma 'imersão digital' que permitiu às pessoas continuarem a comunicar e às organizações manterem o negócio, ainda que de forma limitada. O 'reverso da medalha' foi um aumento preocupante dos ciberataques. Mas, se a segurança online não se consegue garantir a 100%, há medidas para prevenir e mitigar vulnerabilidades.

A CONCLUSÃO é do Webmorning APDC sobre "Cibersegurança em Contexto de Teletrabalho, o primeiro evento no novo formato digital adotado pela APDC para responder aos novos tempos de pandemia e de confinamento, que decorreu a 22 de abril. Desta forma. A Associação mantém o debate e a reflexão sobre os temas que marcam o mercado, dando continuidade ao seu Plano de Atividades, agora reformulado, como reforçou no início do evento o Presidente da Associação.

Fazendo um paralelo com outras pandemias que acontecerem na história, Rogério Carapuça destacou que "uma das grandes diferenças é termos hoje dispositivos tecnológicos que nos mantêm sempre em contacto. Podem permitir não só um fluxo de informação entre todos nós, em simultâneo e entre todo o mundo, mas também a continuidade dos negócios e até a criação de novos". Mas, "não há nenhum avanço tecnológico que não tenha os seus riscos e temos de estar preparados para lidar com eles", com destaque para a cibersegurança.

E o número de ataques online está a subir ao nível global, vindos não só de grupos de crime organizado, com objetivos políticos ou financeiros, entre outros, mas também de grupos de hacktivistas, que são dos que mais crescem. Mas os ataques vindos de dentro das empresas e organizações também provocam grandes estragos, quer por falta de awareness dos seus colaboradores, quer por outros incidentes de segurança relacionados até com parceiros e clientes. O alerta foi dado por Sérgio Martins, Associate Partner da EY.

Salientando que "estamos todos a aprender com esta nova realidade de teletrabalho", o gestor abordou o tema do "Estado de maturidade da Segurança da Informação" e as conclusões do mais recente Global Information Security Sur-

vey (GISS), da EY, realizado ainda antes da pandemia. Este revela que entre os principais alvos dos atacantes estão os dados dos clientes, assim como dados financeiros, propriedade intelectual e dados dos colaboradores.

ATENÇÃO REDOBRADA É PRIORIDADE

Com a pandemia, verifica-se um acelerar constante do cibercrime, através da utilização de inúmeros alvos ligados à COVID-19. E os objetivos são vários, desde a monetização até fins políticos. Trata-se de uma tendência global, porque se vive "uma situação peculiar" que está a ser explorada pelos atacantes: não só as pessoas estão muito mais vulneráveis, como também as organizações, apesar de muitas delas estarem a trabalhar com serviços mínimos.

E não vale a pena ter ilusões de que a situação poderá acalmar, citando o caso do acordo dentro da comunidade de dark web, com a realização de um pacto de não agressão entre as entidades de crime organizado, no sentido de não se fazerem durante esta fase tão crítica ataques a alvos ligados à pandemia. O pacto durou apenas umas horas, findas as quais os ataques voltaram a multiplicar-se, explorando "a realidade das pessoas e das empresas, muitas delas a trabalhar já em modo de contingência, com serviços mínimos, estando muito mais propensas a pagar o resgate do que numa situação normal".

Sérgio Martins antecipa ainda que se poderá assistir, numa segunda fase, a ataques de grupos hacktivistas a crescer exponencialmente. Mas tudo dependerá da resposta das empresas em relação ao impacto económico que a pandemia terá: "se a opção for por muitas situações de lay-off ou despedimentos massivos, os grupos de hacktivistas vão intervir bastante".

Por todos estes motivos, "temos de ter atenção redobrada. São tempos de muita dinâmica, em

que a temática da cibersegurança nunca foi tão relevante para as organizações", até porque a generalidade não estava preparada para trabalhar num ambiente de trabalho remoto e não tinha as adequadas ferramentas. Acresce a falta de awareness dos colaboradores ou o seu descontentamento, em alguns casos, que leva à utilização de equipamentos pessoais no acesso remoto ou a protelar atualizações de segurança.

"A parte das pessoas continua a ser o elo mais fraco. Investe-se muito em tecnologias e processos, mas a componente das pessoas continua a ter de ser trabalhada", salientou o responsável da EY, deixando claro que a adoção massiva do teletrabalho nas últimas semanas está a criar enormes pressões sobre as equipas de IT e novos desafios.

O estudo da EY mostra que 14% das organizações se baseiam apenas em cláusulas contratuais para gerir as redes de terceiros, sem haver qualquer tipo de inspeção, auditoria ou validação sobre se os terceiros estão a fazer exatamente o que está definido nos requisitos de segurança. "É uma das áreas onde temos visto mais risco", alertou.

Assim, e para se mitigar os riscos de segurança no teletrabalho, terão se se "implementar soluções robustas, com colaboradores, clientes e fornecedores, que garantam que as ferramentas que necessitam para trabalhar estão disponíveis e em modo seguro". Mais: "é preciso considerar a segurança um elemento chave nas organizações". Temas como a gestão de identidades e acessos baseada em função ou localização, a autenticação em dois fatores ou a criação de um canal de informação oficial, evitando a desinformação dentro da organização, são por isso críticos.

A cibersegurança nunca foi tão relevante para as organizações. A generalidade não estava preparada para trabalhar num ambiente de trabalho remoto e não tinha as adequadas ferramentas. Acresce a falta de awareness dos colaboradores

O Diretor da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária, Carlos Cabreiro, confirma que a realidade do cibercrime em Portugal tem evoluído substancialmente e até mesmo de forma exponencial, em alguns momentos. Salientando os vários tipos de crime informático e crime que usa os meios informáticos, assim como as diferenciadas motivações, desde o gozo pessoal até ao lucro e às motivações políticas ou religiosas, destaca que, apesar do "caminho sério que tem sido feito", o que estes tempos de exceção têm mostrado é "a ausência de uma cultura de segurança".

CULTURA DE SEGURANÇA PRECISA-SE

"De um momento para outro, quase toda a população está em teletrabalho e teve de se adaptar a uma realidade a que não estava habituada", diz, adiantando que que as preocupações

Ter uma sólida política de backups, segmentar a arquitetura de rede e realizar atualizações permanentes são medidas defendidas pelo orador da PJ para garantir maior segurança das empresas no mundo online

com a segurança estão também a motivar "um aumento exponencial de participações efetuadas de cibercrime à PJ". No último mês, estima-se ter-se registado um aumento da ordem dos 100% em termos de criminalidade online denunciada.

Entre as áreas que mais preocupam no cibercrime estão o phishing, uma realidade que cresceu exponencialmente, com campanhas direcionadas de ransomware e malware. Há uma incidência muito clara do phishing sobre dispositivos móveis, uma vez que são usados por toda a gente. Mas há também muitos ataques vocacionados e direcionados às empresas e organizações, sobretudo de ransomware, assim como o aproveitamento das vulnerabilidades nas VPN's, outro perfil que tem surgido com a massificação do uso do trabalho online e à distância.

Perante esta realidade, o responsável da PJ destaca a necessidade de adoção de medidas como ações preventivas, como uma sólida política de backups, ou a segmentação da arquitetura de rede ou ainda a realização de atualizações permanentes.

Salienta que a PJ tem respondido, desde o

Sérgio Martins,
Associate Partner, EY

"A adoção massiva do teletrabalho criou pressões grandes nas equipas de IT e novos desafios, porque muitas organizações não estavam preparadas para trabalhar num ambiente de trabalho remoto"

"Vivemos uma era de grande transformação e acreditamos que nos próximos tempos haverá muitos projetos de transformação digital. A cibersegurança deve ser envolvida desde o início e não no fim. É preciso considerar a segurança um elemento chave nas organizações"

Carlos Cabreiro,
Diretor da UNC3T- Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, Polícia Judiciária

"Não há dúvida que temos feito um caminho sério no que deve ser a cibersegurança. Mas o mais importante que este período tem revelado é a ausência de uma cultura de segurança. De um momento para outro, quase toda a população que está em teletrabalho teve de se adaptar a uma realidade a que não estava habituada"

"Durante o último mês, tivemos aumentos da ordem dos 100% na criminalidade denunciada. As pessoas estão confinadas, a usar tecnologia, e tudo o que lhes parece matéria suscetível de constituir crime é denunciado"

arranque da pandemia, a perfis completamente distintos de ataques, desde infraestruturas críticas, como aconteceu nos casos da EDP e Altice, até a um perfil de criminalidade mais básica, que afeta os cidadãos, como as falsas campanhas de donativos, por SMS ou por mail. Ou ainda ataques às plataformas de ensino ou de reuniões virtuais, onde o móbil do crime é o mero gozo ou brincadeira, mas que está a levar a uma contínua adaptação e atualização das ferramentas de segurança dessas plataformas. Mas o responsável da PJ assegura: "tenho que ser otimista e dizer que este confinamento e o teletrabalho e teleensino trouxeram também oportunidades, porque vieram criar uma maior cultura de segurança a todas as pessoas" .

As pessoas e empresas estão a ser atacadas de todas as formas, pelo que o trabalho dos hackers bons assume uma relevância crescente num mundo cada vez mais online

O tema das boas práticas para a promoção de uma cultura de cibersegurança nas organizações foi abordado em detalhe pela coordenadora do departamento de Desenvolvimento e Inovação do Centro Nacional de Cibersegurança. Isabel Batista não tem dúvidas de que, "num contexto de teletrabalho, existe um quadro de ameaças muito específico e que os colaboradores são muitas vezes os principais responsáveis pelos ciberataques à sua organização", realidade que resulta frequentemente da falta de cuidado ou desconhecimento, muito mais do que de intenções maliciosas.

Por esta razão, considera que "é no elemento humano que devemos colocar o principal foco da organização. Por mais que estejam apetrechadas das melhores infraestruturas técnicas e da melhor proteção, basta um simples erro humano para colocar tudo em causa", potenciando situações de ciberespionagem, fraude e outras ameaças.

As organizações terão, por isso, que preparar os seus colaboradores para o novo contexto de teletrabalho, dando-lhes formação e dispositivos individuais com os recursos necessários. Ao mesmo tempo, terão de definir quem serão os responsáveis TIC que vão fazer a monitorização, quem é o interlocutor na organização e manter redes de comunicação ativas. Fazer backups regulares e investir em cibersegurança, nomeadamente numa equipa de resposta a incidentes, serão outras medidas a tomar, na sua opinião.

PREVENIR E IDENTIFICAR, CORRIGIR E RESPONDER

Por sua vez, os colaboradores terão de adotar comportamentos mais seguros. Aqui, destaca-se a utilização preferencial de dispositivos autorizados pela organização, sendo sempre os únicos a utilizá-los, assim como usar apenas pens USB confiáveis e ativar o bloqueio automático dos dispositivos com passwords fortes. Utilizar

Isabel Batista,

Coordenadora do departamento de Desenvolvimento e Inovação, Centro Nacional de Cibersegurança

"Face ao contexto de teletrabalho, existe um quadro de ameaças muito específico. Os colaboradores, voluntária ou involuntariamente, são muitas vezes os principais responsáveis por ciberataques à sua organização"

"É no elemento humano que devemos colocar o principal foco da organização. Por mais que as organizações estejam apetrechadas das melhores infraestruturas técnicas, da melhor proteção, basta um simples erro humano para colocar tudo em causa"

André Baptista,

Founder da PENTHACK & Bug Bounty Hunter & Professor Assistente Convidado no Mestrado em Segurança Informática da FCUP

"Basicamente, precisamos de saber prevenir e identificar, corrigir e responder. As equipas de IT têm de ter especial cuidado, identificar ameaças, analisar as infraestruturas e até adquirir conhecimentos de hacking. Colocarmo-nos na posição do atacante leva-nos a uma defesa muito mais eficaz"

"A segurança não é perfeita. É impossível alcançar 100% de segurança nos nossos sistemas nas nossas empresas, a não ser que a usabilidade fosse nula. O futuro é imprevisível neste momento"

filtros no ecrã dos portáteis, ter cuidados nos sistemas e nos dados, assim como na navegação, são outros comportamentos aconselhados.

Ainda assim, a segurança online não é perfeita nem se consegue nunca assegurar a 100%. Quem o garante é André Baptista, especialista em segurança informática, que foi considerado em 2018 o melhor hacker do mundo. O último orador deste primeiro Webmorning da APDC não tem dúvidas de que "o futuro é imprevisível neste momento. Estamos numa fase de transição e a segurança poderá resultar em implicações muito mais profundas nesta nova era do que imaginamos. Cabe-nos a todos colaborar e proteger as empresas e organizações, assim como as pessoas, clientes, parceiros e até nações, na sua existência na dimensão digital".

A pandemia e o isolamento social consequente, que levaram a uma utilização massiva do digital por todas as pessoas, tem vindo a potenciar, segundo este perito, um aumento de relevância do hakctivismo. Assim como dos hackers maliciosos e dos jovens curiosos, que estão a aproveitar para explorar a sua criatividade tecnológica.

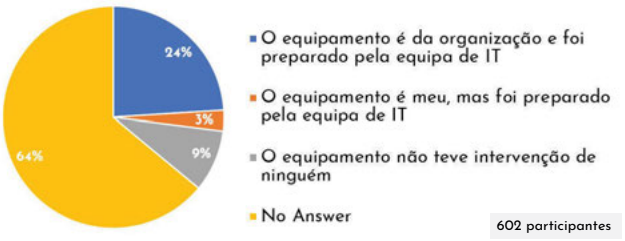
Resultado: pessoas e empresas estão a ser atacadas de todas as formas, pelo que o trabalho dos 'hackers bons' assume uma relevância crescente. E cita os casos dos emails fraudulentos, o sequestro de passwords e pedidos de resgates, as SMS alegadamente de bancos, com replicas de sites que estão cada vez mais parecidas com os sites originais. Nas empresas, "tudo o que é colocado na dimensão digital também constitui uma superfície de ataque muito relevante".

Para André Baptista, a prática corrente das grandes empresas ao nível internacional, quando se trata do trabalho dos especialistas em descobrir falhas de segurança é a recompensa pelo seu trabalho. E defende que esta aposta terá de ser alargada às demais organizações. "Existem hackers que têm boas intenções e que gostam de ajudar e não de destruir. E haverá cada vez mais hackers deste género", garante.

Para este perito, "uma vulnerabilidade é algo de precioso e se for crítica, que pode destruir o negócio. Devemos olhar para ela de modo sério e ter especial cuidado para a corrigir o mais rápido possível". Por isso, "basicamente, precisamos de prevenir e identificar, corrigir e responder".

E não tem dúvidas de que a adoção de serviços cloud pelas empresas oferece "grandes vantagens em termos de segurança, principalmente no que toca ao alojamento, gestão de utilizadores, permissões e todos os mecanismos de segurança inerentes aos serviços cloud. Permitem segmentar muito melhor a rede e seguir as melhores práticas usadas por empresas e organizações de todo o mundo. Garante que os nossos ativos estejam mais seguros e robustos".•

Sobre o equipamento que utiliza em teletrabalho:



Se um hacker enviasse para a sua empresa um relatório que identificasse uma vulnerabilidade crítica, que ação tomava?

Sobre a plataforma de videoconferência que uso:

Que tipo de password usa habitualmente?

Aceda ao vídeo do Evento

https://youtu.be/SXE9gQWuFKg

Patrocinador Institucional

ANACOM – Autoridade Nacional de Comunicações

Patrocinadores Silver

accenture · altice · ALTRAN · ERICSSON · HUAWEI · minsait An Indra company · NOS · vodafone

Patrocinadores Bronze

AXIANS · CGI · CISCO · DELOITTE · DXC TECHNOLOGY · EY · GFI · GOOGLE · HP · HPE · IBM · MICROSOFT · NOVABASE · ORACLE · SAP · SAS

Parceiros

JLM & ASSOCIADOS · NOSSA · VdA · VIATECLA

UPDATE apdc

O UPDATE tem como objectivo disponibilizar informação estruturada sobre cada uma das iniciativas promovidas pela APDC. Pretende-se facilitar, a todos os interessados, um arquivo com os conteúdos mais relevantes de cada evento, que poderá ser consultado em www.apdc.pt