Temática: Conhecer a cibersegurança

O que é a cibercrime?

Desde que existem computadores, existem também cibercrimes. Porém, com milhões de ciberataques e quase mil milhões de vítimas de atividades criminosas online todos os anos, o cibercrime nunca esteve tão alto como agora. Qualquer um pode ser vítima desta atividade, e o facto de todos estarmos virtualmente ligados coloca cada um de nós sob um risco ainda maior.

O termo "cibercrime" pode referir-se a qualquer atividade criminosa que envolva um computador, quer este seja a ferramenta usada no ataque, quer seja o seu alvo. De acordo com o Departamento de Justiça dos Estados Unidos, todos os cibercrimes recaem numa de três categorias:

- crimes que usam computadores como arma (e.g. ataques de hackers);
- crimes que visam um computador ou outro dispositivo (e.g. obtenção ilícita de acesso a uma rede);
- crimes nos quais o computador não é nem a principal arma, nem o principal alvo, mas ainda assim desempenha um papel importante (e.g. armazenamento de ficheiros obtidos ilegalmente).

Com uma disponibilidade da Internet cada vez maior, a natureza do cibercrime evoluiu. Não há muito tempo atrás, grande parte das atividades cibercriminosas envolvia downloads ilegais de conteúdo com direitos de autor, ou discursos do ódio na Internet. Apesar de não poderem ser ignorados, estes atos são praticamente inofensivos quando comparados com o que veio de seguida. Atualmente, novos casos de extorsão, vigilância em massa, roubo financeiro, fugas de dados, roubo de informação pessoal e espionagem são notícia quase todos os dias.

O crimes digital tem tido um crescimento nunca antes visto nos últimos tempos, e por isso não devia ser uma surpresa o facto de a economia mundial estar a perder mais de 500 mil milhões de dólares por ano como resultado de atividades cibercriminosas.

Apesar de muitas agências policiais por todo o mundo estarem a fazer o seu melhor para infligir alguns danos ao cibercrime, esta tendência não mostra sinais de abrandar. Para evitarem a perseguição, alguns cibercriminosos emigraram para países com leis muito permissivas no que toca ao cibercrime e passaram a usar criptomoedas que não deixam rasto em detrimento dos dólares.

Tal como acontece com as atividades criminosas ditas "offline", a maioria dos autores de atos cibercriminosos é motivada por razões financeiras. Mas além do dinheiro, os cibercriminosos também podem ser motivados pelo seu próprio ego, uma causa a que sejam fiéis, vingança pessoal, um desejo de ganhar notoriedade, ou mesmo uma vontade de aumentar o seu estatuto junto dos círculos de hackers.

Fonte: Adaptado de https://softwarelab.org/pt/ 27.Jul.2022.

5 razões para estudar Cibersegurança

Reduzir o risco de exposição de dados confidenciais é uma tarefa básica nos negócios de

hoje, protegendo as informações da empresa na cloud da forma mais eficiente possível. O facto é que os ataques aos computadores estão a acontecer cada vez mais rapidamente, o que coloca em risco a integridade de qualquer empresa, independente de seu tamanho.

Agora mais do que nunca, depois de muito tempo em que tivemos que nos adaptar às possibilidades da tecnologia nos nossos empregos, estarmos protegidos de ataques deste género é fundamental se não queremos sofrer os temidos crimes cibernéticos, que podem ir desde o roubo de propriedade intelectual até a extração de informações confidenciais comprometedoras ou a remoção de bases de dados inteiras.

De acordo com o Relatório de Crimes Cibernéticos de 2019, publicado pelo Ministério do Interior espanhol, no ano passado foram registrados 218 302 crimes cometidos na Internet somente na Espanha, um número que representa 35,8% a mais que no período anterior (160 729 em 2018) e duplicou as 117 399 reclamações recebidas durante 2017. Estes números permitem-nos referir ao cibercrime como o segundo crime mais comum depois do furto.

Num período de incerteza, em que nos vemos obrigados a mudar os nossos hábitos e a nossa relação com o nosso meio pessoal e profissional, reivindicar a cibersegurança como uma necessidade e uma oportunidade de trabalho que se tornará num perfil imprescindível em qualquer empresa, é almejar com certeza rumo a um objetivo fundamental num mundo no qual a identidade, privacidade e segurança são valores essenciais.

Fique a conhecer 5 razões porque a cibersegurança é um perfil promissor:

1. Ser um "super-herói" do século XXI
Quando, graças a este trabalho, uma empresa conseguir evitar um ataque cibernético, percebe-se que não estamos a exagerar. Existem outras formas de ser um super-herói. Ao efetuar formação em segurança cibernética, permite garantir a segurança de quem a confia, ao criar ambientes seguros para proteger a matéria-prima fundamental em serviços digitais - ou seja, dados, contra hackers e outros cibercriminosos.

2. Aposta num setor cuja procura está no seu auge
Um especialista em scibersegurança é um profissional cada vez mais indispensável. Um especialista nesta área conhece diferentes protocolos, padrões, ferramentas, métodos e até leis para impedir o possível roubo de informações de uma empresa. Empresas e governos em todo o mundo enfrentam um número cada vez maior de ataques cibernéticos, enquanto o número de profissionais dedicados a esta área continua insuficiente. Segundo dados da publicação especializada Cibersecurity Ventures, as ofertas de trabalho em cibersegurança triplicarão nos próximos dois anos.

3. Equacionar um salário à altura
Trabalhar com segurança digital é sinónimo de estabilidade no emprego. O salário médio de um especialista em cibersegurança está entre 30000 e 60000 euros por ano, dependendo da responsabilidade e do nível de especialização. Os números mais altos estão associados a gerentes de segurança, embora aqueles que optam por opções como administração de segurança de sistema e redes, consultoria de segurança e hacking ético ou gestão de proteção de dados não ficam assim tão atrás.

4. Desenvolver competências que muito poucas pessoas conhecem
Tendências tecnológicas como Bring Your Own Device (BYOD), Cloud Computing, Big Data, Internet das Coisas ou aplicações móveis exigem formação e soluções que representam desafios reais para os profissionais de tecnologia. Saber como responder de forma adequada à segurança de serviços e aplicações como esses vai transformar em um especialista versátil em que as empresas vão querer depositar sua confiança e sigilo.

5. Cibersegurança é um trabalho entusiasmante
Aprender a colocar no lugar dos outros e saber ouvir, conhecer os seus problemas e fornecer as melhores soluções. Também educar as equipas de trabalho no uso adequado dos dispositivos para evitar imprevistos (por ex: empresas de alto

nível). Enfrentar desafios entusiasmantes e desafios contínuos - no fundo, ser a melhor defesa da sua equipa. É necessária saber responder à questão. Tens coragem de garantir a privacidade e a segurança em grandes empresas? Se sim, opta pela cibersegurança e não deixes que os hackers coloquem os serviços digitais das pessoas com quem trabalhas numa encruzilhada.

Fonte: Adaptado de https://www.ironhack.com/pt/ 28.Jul.2022.