03

© Nicolau

Cyber: this risk is real and needs to be managed

Cibersegurança: o risco é real e é preciso geri-lo

Paulo Moniz, Director of Security, EDP Information Systems Department, explains how the Portugese power group manages its cyber risk and urges all business and risk managers to take the exposure, its prevention and management very seriously. This is no media hype, argues Mr Moniz.

Paulo Moniz, Diretor de Segurança da Direção de Sistemas de Informação da EDP, explica o modo como o grupo português do setor da energia gere o risco cibernético e recomenda fortemente a todos os gestores de risco e empresas que tomem em séria consideração a exposição ao risco, a tomada de medidas preventivas e gestão do mesmo. "Não se trata da mediatização excessiva de um mito", afirma.

To say that organisations and individuals are constantly facing threats to their cybersecurity is old news and will come as a surprise to no one. Reports about cyberattacks can easily be found online with just a few clicks of your mouse or, in more traditional fashion, by leafing through a newspaper. However, if we consider that many organisations choose not to divulge breaches of their security, whether because they fear the loss of customer confidence or because they are not subject to legislation that obliges them to do so, we may assume that the reality is considerably more dramatic than the public facts suggest.

In this increasingly worrying scenario, there is an urgent need for organisations and individuals to have a clearer idea of the cyber risks they face and the measures they need to adopt to mitigate them, in accordance with what the organisation deems to be an acceptable level of risk. The protective measures must ensure a perfect balance between the company's need for protection and the requirements that will enable it to offer a streamlined and efficient response to the demands of the market in which it operates.

In addition to its size and global presence, the EDP Energias de Portugal Group is responsible for systems that control crucial infrastructures in various geographies. This fact implies that the organisation's cyber risk is relevant and complex. It can and does have a potential impact on the group's strategy and operations because an attack on its systems could have consequences both from an organisational perspective (operations, company image and financial repercussions) and from the point of view of the society that it serves. The bottom line is that a threat to national security could ensue.

The way in which EDP approaches and manages cybersecurity risks involves firstly the definition of a governance model for information security that is aligned with the EDP group's strategy. This approach implies the need to define protection policies on the basis of their strategic goals and, consequently, the criticality of the assets to be protected. This means, for example, that security policies would be less restrictive in office networks, where the productivity and efficiency of the staff is the focus of the information system, than they would in crucial infrastructures where the security and sustainability of our society could be at risk. It is important to note that the dizzying pace of technological evolution means governance must be constantly updated in terms of security. This has to be done to help address new paradigms such as Cloud or Bring Your Own Device services.

Another fundamental aspect in cyber risk management is the need to align such policies with effective technological means for prevention and detection. In this respect, EDP has invested heavily in technological solutions that will enable the protection of the perimeter and the detection of security incidents. A security monitoring hub has been created in the form of the SOC EDP – Security Operation Centre. This Centre collates events from the various technological infrastructures and applications, and correlates

Mencionar que as organizações e indivíduos estão sujeitos a constantes ameaças à sua cibersegurança deixou de ser novidade ou mesmo razão para surpresa. As notícias sobre ataques informáticos estão à distância de uma procura na *internet* ou do tradicional folhear de um jornal. Contudo, se considerarmos que muitas organizações optam pela não divulgação das suas quebras de segurança, quer por receio de perderem a confiança dos seus clientes, quer pelo facto de não estarem sujeitas a legislação que as obrigue a divulga-las, podemos inferir que a realidade é consideravelmente mais dramática do que os factos sugerem.

Neste cenário cada vez mais preocupante, torna-se premente a necessidade das organizações e indivíduos terem uma noção mais precisa dos riscos cibernéticos e, de acordo com nível de aceitação de risco definido pela organização, quais as medidas que necessitam adotar para a sua mitigação. Estas medidas de proteção deverão habilmente balancear a necessidade de proteção da empresa com os requisitos que lhe permitam responder com flexibilidade e eficiência às exigências do mercado onde atua.

O Grupo EDP Energias de Portugal, para além da sua dimensão e presença global, tem sob sua responsabilidade sistemas que controlam infraestruturas críticas em diversas geografias. Este facto implica que o risco cibernético da organização é relevante e complexo, com impactos na sua estratégia e atuação, considerando que um ataque aos seus sistemas pode ter consequências tanto no plano organizacional (operacional, de imagem ou financeiro), como na sociedade que serve, passando o impacto para o estatuto de ameaça à segurança nacional.

A forma como a EDP enfrenta e gere estes riscos de cibersegurança passa em primeiro lugar por definir um modelo de *governance* de segurança de informação alinhado com a estratégia do Grupo EDP. Esta abordagem implica a definição de políticas de proteção consonantes com os seus objetivos estratégicos, e por conseguinte com a criticidade dos bens a proteger, o que leva a determinar, por exemplo, políticas de segurança menos restritas em redes *office*, onde a produtividade e eficiência dos colaboradores é o foco dos sistemas de informação, do que as políticas existentes nas infraestruturas críticas, onde poderá estar em causa a segurança e sustentabilidade da nossa sociedade. É importante referir que a vertiginosa evolução tecnológica exige uma constante atualização da *governance* em termos de segurança para contemplar novos paradigmas como os serviços na *Cloud* ou *Bring Your Own Device*.

Outra vertente fundamental na gestão deste risco assenta na materialização das políticas com meios tecnológicos efetivos de prevenção e deteção. Neste aspeto a EDP tem feito um forte investimento em soluções tecnológicas que permitam a defesa do perímetro e a deteção de incidentes de segurança. Foi criada uma valência de monitorização de segurança traduzida no SOC EDP – *Security Operation Center*, que recolhe eventos das diversas infraestruturas tecnológicas e aplicações, correlacionando-as de modo a identificar padrões que possam criar alertas para possíveis incidentes de

them in order to pinpoint patterns that could alert us to potential security incidents. EDP also conducts continuous ethical hacking tests in order to detect security vulnerabilities in timely fashion.

In terms of prevention, a fundamental aspect for the mitigation of cyber and regulatory risk is that of the management of identities and access to the EDP group's information resources. By means of a process and a unique tool, the life cycles of approximately 19,000 identities and accesses to over 40 information resources, such as applications and directories and the like, can be managed.

Despite the robustness and effectiveness of the measures that can be implemented, it is important to be aware that, at some point in the future, a cyberattack is bound to breach all the defences that have been built. When this happens, the criminals will have successfully achieved their goal by compromising the confidentiality of our information or even the operational capacity and availability of the systems that support the business. At that point, it would be vital to react and analyse, and in this scenario resilience will be the principle to adopt. We intend to achieve this by ensuring that the resources that operate crucial control systems are capable of responding. This involves the provision of training in cybersecurity, changing attitudes and behaviour by means of awareness raising campaigns on our internal channels (Corporate TV and radio, in-house magazine and Intranet) and, in particular, by designing business continuity plans, which are key in such scenarios. It should be stressed that these plans are the responsibility of all EDP Group companies. However, the continuity of IT services and, in particular, the Disaster Recovery solution implemented, play a central role in EDP's resilience, in light of the ever-increasing dependency on information systems.

All of the above factors, which encompass the phases of prevention, detection, reaction and analysis, translate into EDP's approach to the issue of cyber risk management. However, we feel that we need to take a more formal approach with our cyber risk management efforts and have therefore started an IT Risk project to produce a risk map and a risk management process.

We are hoping that this project will allow us to achieve improved decision-making on IT management and, in particular, IT security, by incorporating the quantification of risk in the decision-making processes. We are also expecting to achieve better quality reporting to senior management. This would lead to

segurança. Ainda dentro desta vertente realizamos testes contínuos de *ethical hacking* de modo a poder detetar atempadamente vulnerabilidades de segurança.

Também ao nível da prevenção, um tema fundamental para a mitigação do risco cibernético e regulatório relaciona-se com a gestão de identidades e acessos aos recursos de informação do Grupo EDP. Através de um processo e de uma ferramenta única é gerido o ciclo de vida de cerca de 19000 identidades e os acessos a mais de 40 recursos de informação (aplicações, diretórios, etc.).

Apesar de robustez e efetividade das medidas que se possam implementar, é importante ter a consciência de que inevitavelmente algum dia um ataque cibernético terá a capacidade de ultrapassar todas as defesas implementadas e que a entidade criminosa alcançará com sucesso os seus objetivos, ao afetar a confidencialidade da informação ou mesmo a operação e disponibilidade dos sistemas que suportam o negócio. Importa nesta fase reagir e analisar, sendo que neste cenário o princípio que adotámos é a resiliência. Pretendemos alcançá-la com a capacitação dos recursos que operam sistemas de controlo críticos, providenciando treino em cibersegurança, pela mudança comportamental, através de ações de sensibilização pelos canais internos (Corporate TV e Rádio, Revista e *Intranet*) e em particular pelo desenho dos planos de continuidade de negócio, fulcrais nestes cenários. É relevante salientar que estes planos são da responsabilidade das empresas do Grupo EDP, no entanto, dada a crescente dependência nos sistemas de informação, a continuidade de serviços IT, e em particular a solução de *Disaster Recovery* implementada, assumem um papel central na resiliência da EDP.

Todos os fatores citados, que abrangem as fases de prevenção, deteção, reação e análise, traduzem na realidade a forma como a EDP faz a gestão do risco cibernético. Sentimos porém a necessidade de dotar de um carácter mais formal esta atividade, pelo que iniciámos um projeto de Risco IT, como o objetivo de produzir um mapa de riscos e um processo de gestão dos mesmos. É nossa expetativa atingir com este projeto uma melhoria na tomada de decisão em relação à gestão de IT, e à sua segurança em particular, incorporando nos processos de decisão a quantificação do risco. É também expetável uma maior qualidade do *reporting* à gestão de topo, conduzindo à tomada de decisões mais fundamentada, que poderá permitir enveredar por outras opções de gestão do risco, como a viabilização de mecanismos de transferência de risco.

better-informed decision-making and could allow us to embark on other risk management pathways, such as the enablement of risk transfer mechanisms.

The reality of cybersecurity threats and cyber risk, in particular, is far from virtual and is a serious concern. Only a strong sense of responsibility, commitment and collaboration by organisations from different sectors, operators, insurance companies, universities, the military, politics, justice, police forces, manufacturers and the like, will enable us to stand up to this intangible but very real cyberthreat. Such a collective effort will also give us all the confidence that the world of information, opportunities and global knowledge that we see expanding frenetically around us will help create a society with a safer, more trustworthy and more sustainable future.

As ameaças à cibersegurança e o risco cibernético em particular, são uma realidade muito pouco virtual e deveras preocupante. Só com um grande sentido de responsabilidade, empenho e colaboração das organizações de diferentes sectores (operadores, seguradoras, académicos, militares, politicas, justiça, policiais, fabricantes, etc.) será possível fazer frente a esta intangível mas muito real ciberameaça e ter confiança que o mundo da informação, oportunidades e conhecimento global que vemos freneticamente crescer à nossa volta, corresponderá efetivamente a uma sociedade com um futuro mais seguro, confiável e sustentável.

Paulo Moniz
EDP GROUP – DIRECTOR FOR INFORMATION SECURITY AND IT RISK

With 18 years' experience in the world of information technology, Paulo Moniz began his career as systems administrator at EDP Distribuição before moving to EDINFOR, where he was involved in various international development projects as analyst, programmer and trainer. He later took on project management functions, having turned his attention to the field of security in 2008 when he took over leadership of Security Practice at Logica Iberia. Since 2010, he has been Director for Information Security and IT Risk at the EDP Group.
Paulo completed his Degree in Electrical and Computer Engineering at the University of Lisbon's Engineering School, Instituto Superior Técnico, in 1995. He later did a Postgraduate Degree in Information Systems at the same institution. He also has an MSc in Information Security from Carnegie Mellon University and a Master's in Information Security from Lisbon University's Faculty of Sciences.

Com uma experiência de 18 anos no mundo das tecnologias de informação, iniciou a carreira como administrador de sistemas na EDP Distribuição, tendo posteriormente transitado para a EDINFOR onde participou em diversos projetos internacionais de desenvolvimento de soluções como analista, programador e formador. Mais tarde assumiu funções de gestão de projeto tendo abraçado a área de Segurança em 2008, quando assumiu a liderança da Security Practice na Logica Iberia. Atualmente, desde 2010, é diretor pela área de Segurança da Informação e Risco IT no Grupo EDP.
Concluiu em 1995 a licenciatura em Engenharia Eletrotécnica e de Computadores pelo Instituto Superior Técnico tendo mais tarde concluído uma Pós Graduação em Sistemas de Informação (POSI) na mesma instituição. Possui também um MSc em Information Security pela Universidade de Carnegie Mellon e um Mestrado em Segurança Informática pela Faculdade de Ciências da Universidade de Lisboa.