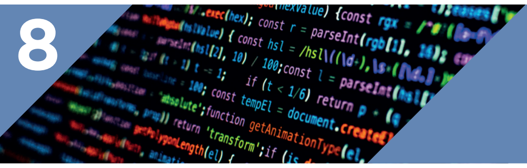
Best practices for digital security: what can companies do?

LEONARDO

		GUIDELINE	PUTTING IT INTO ACTION
1		Create awareness with all staff	Inform and train company staff on the risks and vulnerabilities that the new situation could bring, the risk behaviours to avoid, and the right ones to adopt responsibly.
2		Use company devices as much as possible	Whenever possible, use company devices which when compared to domestic ones are more secure and have appropriate protocols to avoid data leaks and possible intrusions.
3		Update securityof company devices frequently	Keep company devices updated, ensuring they have the latest security patches, adequate Smart Working antiviruses and EDR (End Point Detection & Response) systems.
4		Intensify use of vulnerability management tools	Respond to new security needs by intensifying the frequency of perimeter and internal monitoring and scanning, using vulnerability management tools to identify possible threats.
5		Update perimeter protection devices	Verify that the VPN gateways and perimeter protection devices in general, are updated with the latest version, and the latest patch made available by the vendor. Also eliminate services and features not needed, and use secure protocols for encryption and strong “cypher suites”.
6		Limit usage and functionality of company hardware devices to work activity only	Plan correct device hardening by imposing usage and functionality limits on the company hardware by configuring it in order to prevent it being used for reasons other than work.
7		Virtualise desktops	Apply desktop virtualisation techniques (VDI) by adopting solutions that allow virtualised assets.
8		Encrypt data	Provide local data encryption systems (File System/Disk Encryption) in order to prevent the loss of critical data.
9		Use only Virtual Private Network (VPN) connections	Use encrypted connection only (VPN) to connect to company network by using “cypher suites” with the appropriate strength.
10		Take measures to mitigate volumetric attacks	Opt for anti DDoS (Distributed Denial of Service) solutions in order to be ready to mitigate any volumetric attacks aimed at saturating the communication band of the victims.
11		Report vulnerabilities promptly	Choose early warning solutions for the timely communication of all threats that smart working is particularly exposed to (boundary protection, VPN gateway, workstation and endpoint).
12		Adopt guaranteed continuity communication solutions	Implement solutions that involve the use of various providers for communication services (multi-carriers) to guarantee service continuity provided by the people who are working remotely.