INFORMATION / CYBER SECURITY

THREATS AND APPROPRIATE SECURITY CONTROLS

<u>Забележка:</u> В следващата таблица са показани **10 (десет) основни заплахи** за информационната сигурност и съответните за тях, подходящи набори от контроли за противодействие. Подробно описание за съответните заплахи / контроли, може да се намери в съответните безплатни курсове, публикувани в платформата за асистирано самообучение **InfoSec Learning Management System.**

THREATS	Advanced Persistent Threats (APT)	Cybercrime	Distributed Denial of Service (DDoS)	Insider Threats	Malware	Mobile Malware	Ransomware	Social Engineering	Unpached Systems	Watering Hole
SECURITY										
CONTROLS										
ARCHITECTURE										
Defense-in-Dept	Х	X	Х	Х	Х	X	X	X	Х	Х
Device Level Hard & Soft Controls	Х	Х			X	Х			X	
Endpoint Controls			Х	X	X	X	X		X	
Network Infrastructure		X	Х						Х	
Log Management	Х	X	Х	Х	Х	X	X	X	Х	Х
Perimeter Controls		X	X			Х				
User Management Awareness	X	X	X	X	X	X	X	X	X	X
DATA MANAGEMENT										

Access Control		Х								
Data Integrity	Х	X	X				Х			
Data Privacy	Х	X			Х	X	X			Х
Data Retention / Disposal	X	X	X				X	X		
Data Validation	Х	X								
Digital Rights Management	X	X		X						
Classification		X						X		
Encryption	X	Х			X	X	X			X
Manipulation Controls	Х	Х		Х			Х		X	
HARDWARE										
Access Control on Device Level				X			Х		X	
Asset Register	X	X	X	X	X	X		X	X	X
Backup Management						X			X	
BYOD Management / Policy	Х	X		X	X	X	Х			
Facilities / Data Centers Management									X	
Retirement / Disposal Lifecycle		X								
Maintenance									X	
Mobile Device Management				X	X	X	Х			
Monitoring	X	X	X	X			X		X	
Patch Management			X		X		X			
Retirement / Disposal Lifecycle									X	
Supply Chain Management		X	X							
Support Agreements	Х	Х					X			
Testing and Certification			X							
NETWORK										
Access Control	Х	X						X		

Anti Virus / Malware	X	X		X	X	X	X		X	
Application Layer Firewalls / Security Proxy	Х	X	Х		X	х	X		X	X
Authentication		X								
Change Management				Х						
Configuration Management and Hardening	Х		Х	Х	X	х	Х		X	
Denial of Service Protection			X							
DLP (Data Loss Prevention)	Х	X	X	Х	X	Х	X		X	Х
Encryption		X								
Honeypots		Х	Х						Х	
Monitoring / Correlation System			X	X					X	
Network Resilience		X	X		X	X				X
IPS / IDS (Intrusion Prevention / Detection System)	Х		Х		X	Х	X		X	
Patch Management	Х	X	Х	Х	Х	Х	X	X	X	Х
Remote Access Controls	Х	X	X	X		Х			X	
Secure Link	X	X				X			X	
Segmentation	X	X	X	X	X	X	X		X	X
Situational Awareness				X				X	X	
Traffic Management / Filtering	Х		X		X	Х	X		X	х
Vulnerability Scanning	Х	X	X	X	X		X		X	
SOFTWARE										
Access Control				Х	X				X	
Authentication				Х					X	
Authorization				Х					X	
Backup / Archival					X		X			X

Change Management				X						
Inventory Management		X								
Patch Management				X	X	X	X			X
Security Awareness		X	X	Х	Х		Х			Х
Source Code Management		X	X	X						X
Secure Software Architecture			X	X						
Testing			X							
USER										
MANAGEMENT										
Access Control		X		X			X	X	X	
Employment Lifecycle	X	X					Х	X		
Identity Management		X						Х		
Multifactor Authentication	X	X		X			X			
NDA / Confidential Agreement / Deterrent Policy		X		Х						
Responsibility Management				Х					X	
Security Awareness					X					
Security Awareness Training	X	X	X	Х	X	X	X	X	X	X
Segregation of Duties	X	X	X	X	X	X	X	X	X	X
Third Party Management		X	X	X			X	X		
User Credential Life Cycle Management								X		
User Reconciliation	X	X		X			X	X	X	