The Ultimate Cyber Security Checklist to Protect Your Organization During Coronavirus Pandemic

Purpose of This Document

The global Coronavirus crisis implements a quarantine policy that is becoming increasingly difficult for many economies. This policy, in turn, causes cyber attacks targeting remote connection credentials and vulnerable personal devices and unprotected endpoints. This chaotic situation puts a heavy burden on the shoulders of Chief Information Security Officer (CISO). This template is designed to be concise, clear, and actionable, with all the essential apps to check out to ensure that cyber defenses survive successfully during this difficult time.

This template consists of five parts:

Security Technology: List of products to be installed and configured. The purpose of selecting this category was to examine the data collected from threat intelligence and attack analysis sources.

Security Team: Each team has a set of procedures to routinely conduct ongoing security operations, regardless of size and competence level. These procedures should at least be renewed and updated in many ways to address specific IT and cyber attack changes.

General Workforce: Information Security Managers know better than anyone that the weakest link in security is created by employees rather than machines or applications. The established uncertainty brought by Coronavirus makes people more vulnerable to any kind of social engineering manipulation. It is imperative to raise awareness of your workforce against increasing attacks through awareness, training and security drills.

Outsourcing Service Providers: Regardless of whether your organization performs all security tasks within the company, you should develop a more effective defense strategy by seeking support from experts in the field from an outside perspective.

Management Visibility: Managers of the organization must have regular and complete information about the efforts and security operations of Information Security Managers. Is there an increase in attacks, security teams and products are working as expected, is there a violation, etc. Every Information Security Manager must have the infrastructure to produce these reports effortlessly.

Why We Prepared This Document?

This document has emerged as the result of numerous interactions of SMSK Information Technologies (SecroMix) with Information Security Managers and security organizations. As SMSK (SecroMix), we aim to circumvent this process in a healthy way with the idea that the attackers will want to take advantage of the gap formed during the coronavirus quarantine, they will try to evaluate the current conditions well and will not hesitate to apply various attack vectors. Our goal is to simplify and optimize the protection process of Information Security Managers with an easy-to-use template that can easily adapt to an organization's need.

Secure Remote Work Checklist

Template	Steps	Check
Security Technology	Use MFA for remote connection.	
	Set the security policies of remote devices.	
	Review remote connection authority checks.	
	Enable malware / antivirus protection on devices (business and personal).	
	Set software policies to be installed for devices (Java, Flash, etc.).	
	Secure e-mail.	
	Review or create sign-in policies (based on time, geographic location, concurrent sessions, etc.)	
	Watch events in cloud environments (IaaS + PaaS + SaaS).	
	Enable DDOS protection.	
	Threat intelligence: Check your IP reputation services regularly.	
	Create detailed remote connection policies that potentially restrict access to sensitive resources.	
	Update DLP policies, taking into account unmanaged devices and exposed services. Make sure these policies apply to both on-premises and cloud environments.	
	Update data recovery procedures and make sure your backups are working properly.	
	Monitor your hardware resources.	
	Monitor the instant status of your running services.	
Security Team	Set strict monitoring procedures for remote connection to sensitive resources.	
	Set strict monitoring procedures for connection to cloud environment.	
	Make sure that a well-defined "Incident Response" procedure is available.	
	Identify an ongoing vulnerability management process with a focus on public services.	
	Do not delay emergency patches with vulnerabilities.	
General Workforce	Create and launch a private security awareness program that focuses on phishing, remote credential theft and strong authentication.	
	Define a reliable communication channel and ensure that all employees communicate through these channels.	
	Identify the mutual authentication process among employees.	
	Create periodic security drills against social engineering design emails.	
Outsourcing Service Providers	If any of the above exceeds the capacity of your resources, consider working with a "Managed Security Service Provider (MSSP)":	
	• Security products distribution assistance	
	• Security monitoring and management assistance	
	• Incident Response (IR) team	
	• Information Security awareness trainings of employees and measurement of security levels in certain periods	
Gaps and potential effects explained	Create periodic reports showing below:	
	• Create periodic and on-demand reports that show:	
	• Gaps and potential effects explained	
	• Gaps and potential effects explained	