Cybersecurity Toolkit – 2021

The Ultimate Security Checklist That Every Business Need To Have In 2021

2020 has been a challenging year for everyone - deadly and disruptive viruses changed our way of living from both a biological and a digital perspective.

Fact: More than 4.66 billion Internet users are active as of January 2021 – this represents 59.55% of the world's population[1].

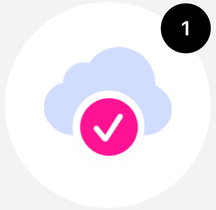
With most businesses operating remotely, hackers stepped up attacks against the expanded and target-rich environment, with breaches that almost doubled from 2019. Online crimes reported to the FBI's Internet Crime Complaint Center (IC3) nearly quadrupled due to the COVID-19 pandemic[2].

Remote working will continue to be the trend this year, and cybersecurity will continue to be a major challenge. Ransomware is also expected to attack a business every 11 seconds by the end of 2021.[3]

For cybersecurity preparedness in 2021, we've created this checklist to help reduce and eliminate the identified threats/vulnerabilities that can probably place your organisation at risk. Implement these critical controls correctly, and you can prevent, detect, and contain the majority of the attacks we've seen in the past year.

[1] Source: https://www.statista.com/statistics/617136/digital-population-worldwide/
[2] Source: https://www.fbi.gov/news/stories/ic3-logs-6-million-complaints-051721
[3] Source: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

The 8 point checklist



1 Patching your software and keeping your OS and applications up-to-date

One of the most cited and most crucial actions you can take is keeping all your software applications, from operating systems to firewalls and routers, up to date with the latest security patches. This is because modern software programs are developed to be resilient against current risks and attacks. Legacy systems often introduce various security challenges and might contain unaddressed vulnerabilities, or their vendors might have stopped supporting them in releasing security updates and patches. Acquiring up-to-date software is vital to enhancing the security of an organization.

2 Use multi-factor authentication (MFA)

Simple usernames and password combinations can easily be compromised. Implementing third authentication factors, such as PIN or biometrics, dramatically enhances security, especially for accounts accessible from anywhere on the internet or arrangements with administrator-level access.

3 Provide and require the use of password managers

Password reuse is reportedly common in 52% of users[4], and these reused passwords can be cracked within 10 guesses. Ensure your employees are using unique solid passwords by providing them with the right tool that works for them and allows them to manage shared passwords across your business efficiently.

[4] Source: https://www.microsoft.com/en-ww/security/business/security-intelligence-report?rtc=1

The 8 point checklist

4

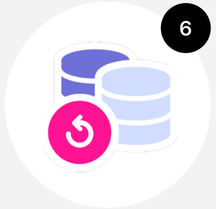
Log alerts and monitoring

Logging and alerting are a crucial part of understanding how an incident occurred and when it started – it's the first step in having visibility of all activity in your environment. Storing and securing your logs in a central place makes log analysis and alerting easier.

5

Secure internet-exposed services

Securing your internet-exposed services requires a combination of other key critical controls - patching, network segmentation, multi-factor authentication, and logging - being applied to internet-exposed services. On top of these critical points, disabling unused and unnecessary internet services running on your system can help reduce the risk of getting your system and your attack surface exposed to threats.



6

Implement and test backups

Restoring your data from backups is one of the best ways to return to business after a cyberattack quickly. Regularly backing up your data to a secure, encrypted, and off-site location can aid in recovery from a cyberattack as well as other human and natural disasters. It's also essential for compliance with certain government regulations.

7

Implement network segmentation

To limit the impact of intrusion, you need to separate and break down your network into smaller segments and set access controls to manage connections across them.

A strategic network segmentation ensures that the most sensitive and confidential data is not accessed. This allows your organisation to set more robust granular security controls on the smaller networks with critical data or systems.

8

Enforce the principle of least privilege

Do not give an account more access than it needs to perform a duty. Restricting access to only what's needed also limits the amount of things an attacker can do if the account is compromised.

To prevent users from accidentally or intentionally making changes that can cause security incidents in your organisation, enforce the principle of least privilege [5] access for accounts, especially for automated processes.

[5] Source: https://en.wikipedia.org/wiki/Principle_of_least_privilege

Get to know more about Putti Apps.

For more information about our cybersecurity consultancy, visit https://www.puttiapps.com/cyber-security-consultancy/.

Visit Us →