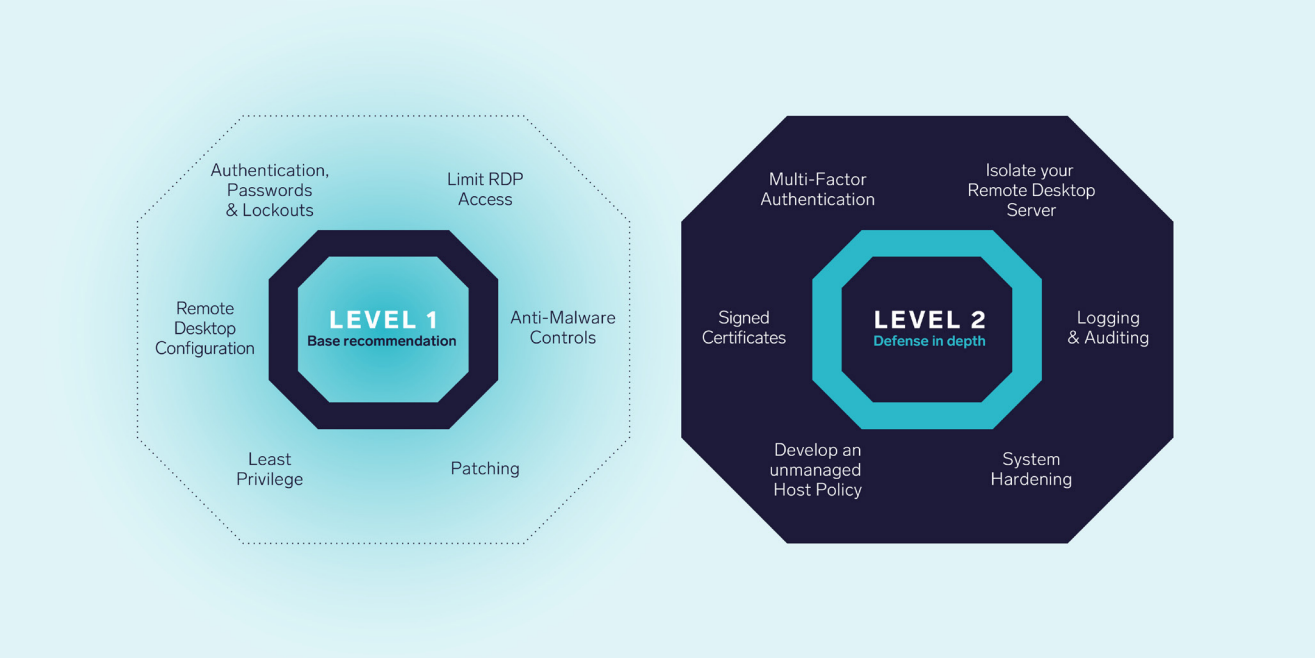
The Covid-19 Crisis & Cyber Security

By Kadir from CyberClan

MARCH 13, 2020

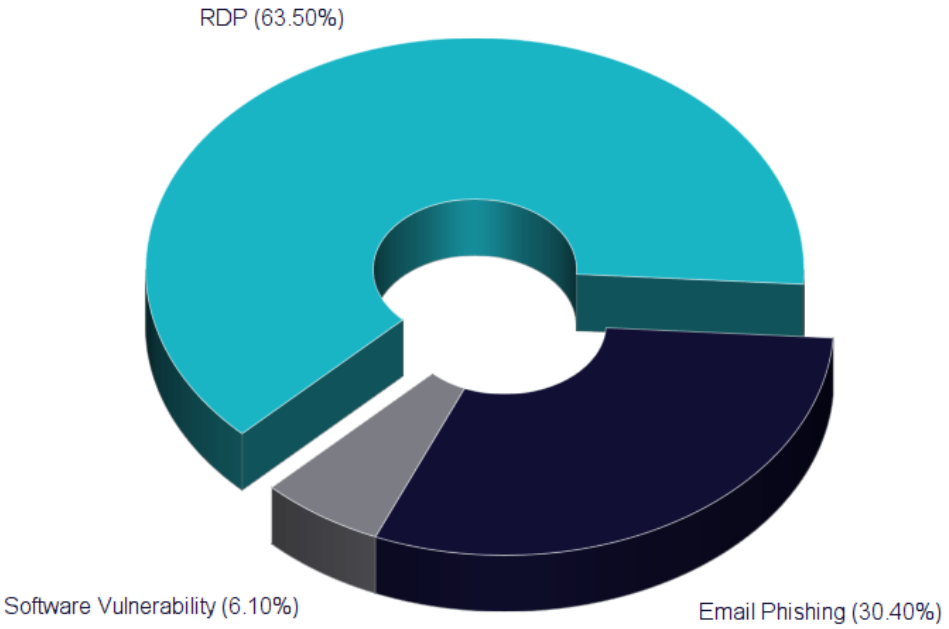


The Covid-19 crisis is having a significant effect on the economy and businesses globally. With the World Health Organisation declaring a pandemic, President Trump is implementing a 30-day travel ban on Europe into the USA. The effect on global companies is significant due to worldwide closures of offices and employees being required to work from home for their safety. The impact on business operations is being felt, and with that immediate impact, we must look at cybersecurity and vulnerabilities that is presenting for each organization.

One of the most important challenges for organizations is keeping your workforce safe and productive. The easiest solution for most employers is to allow staff to work from home but by doing so, businesses are now increasing their exposure for potential cyber-attacks on their networks.

A Remote Desktop Protocol (RDP) is a common tool used to allow remote access to a network and is often used by organizations to allow staff to work remotely. However, the majority of

COMMON ATTACK VECTORS USED BY RANSOMWARE IN Q1 2019



ransomware attacks occur through the exploitation of the use of RDP. Attackers typically gain access to a network by either brute-forcing credentials or sending a fake email (phishing) to get an unsuspecting individual to willingly enter them on an attacker-controlled website. There are even previously compromised credentials for sale on the dark web which can be simply purchased for a few dollars.

So how can you minimize the threat of a network compromise when using RDP?

Here are some tips on facilitating your employees' remote access to work from home in a secure manner.

The Level 1 profile is considered a base recommendation that can be implemented relatively promptly and is designed not to be very cumbersome to an IT Team. The Level 1 profile benchmark intends to lower the attack surface of your organization while keeping the machine functional and not hindering business continuity.

The Level 2 profile is considered to be "defense in depth" and is intended for environments where security is paramount, and a breach of infrastructure cannot be permitted. The recommendations associated with the Level 2 profile are more involved for your IT team to implement and manage – still, in our opinion, the increase in resiliency is very much worth it.

LEVEL 1

Limit RDP Access

Limiting the number of IP addresses and locations that can connect to your RDP server is a critical tool in the defender's arsenal. Restrict access to the server by requiring a VPN to connect. If that's not feasible or possible, whitelist the IP addresses where your users will work from home instead. If you have too many users to do this for, you may instead look at geolocation blocking by only allowing traffic from the countries and regions your users reside.

Anti Malware Controls

Make sure your server and IT team are set up to log and regularly audit security and system events for abnormal activity, protected with a trusted antivirus with tamper protection. This way, when an attacker gets access to the server, they will have difficulty executing malicious code and tools they need to stage their attack successfully.

Patching

Use a recent version such as Windows Server 2016 or 2019 for your RDP server as it supports the latest security controls and mechanisms that aren't present on older versions. Keeping your servers up-to-date with the latest software and security updates should be a key component of your security strategy.

Least Privilege

Make sure only the users that require remote access can log into the server. Deny access to the Remote Desktop Server for all other users, including user accounts, service accounts, and other administrator accounts that do not require access through Remote Desktop. Additionally, users often only require access to a minimal number of files, folders, and resources out of all files that are present on a file server. Configure the roles and permissions on the server in such a way that every user can access nothing more than what they require to do their work.

Remote Desktop Configuration

Configure and require Network Level Authentication ("NLA") and enable the highest level of encryption for your Remote Desktop Protocol configurations. Using strong encryption and NLA further protects against exploitation, traffic interception, and other Remote Desktop Protocol related vulnerabilities.

Authentication, Passwords, & Lockouts

Make sure to enforce a strong password policy of at least 12 characters within your domain environment to reduce the chance of credential re-use and successful brute force attacks. Additionally, adjust the lockout policy to a maximum of 5 lockouts, and increase the lockout time

after five attempts to at least 1 hour. Legitimate users that do lock themselves out should be manually validated and unlocked by the IT team. You may also choose to limit the logon hours for users to accepted business hours.

LEVEL 2

Multi-Factor Authentication

The question is not if, but when an attacker will get their hands on valid credentials. Implementing and requiring Multi-Factor Authentication to log in to the RDP server will significantly increase the complexity of a compromise, and therefore add a noticeable layer of security to your infrastructure.

Isolate your Remote Desktop Server

Place your remote desktop server in a separate area of the network with minimal access to the remainder of the internal resources. This will make it more difficult for an attacker to stage an attack against the internal network in the event that the Remote Desktop Server is compromised.

Logging and Auditing

Make sure your server is set up to generate a rich set of logging data, and that your IT team regularly audits and reviews the logs for abnormal activity. Reviewing audit logs will give a security team real-time information about the state of the server, and often successful breaches could be prevented if the IT team looked at the Indicators of Attack for days that were visible in the audit logs.

System Hardening

Leverage industry-standard hardening templates and controls by accredited security institutions such as the Centre for Internet Security (CIS).

Develop an Unmanaged Host Policy

Ideally, only corporate-controlled machines should be able to authenticate to the corporate network. Unfortunately, it is not always possible to issue corporate laptops to each member of the organization, and the organization may choose to allow users to use their personal devices. When working with unmanaged hosts and personal devices, many uncertainties and risks are introduced into the environment. As these are assets not managed by corporate IT, it is difficult to identify and

control the state these machines are in. An Unmanaged Host Policy covering minimum requirements for personal devices can assist mitigate this risk.

- An up to date personal antivirus solution
- An antivirus scan prior to connecting to the corporate network
- An operating system that is not out-of-support-life (Windows 10, macOS Catalina)

Signed Certificates

Implement signed security certificates on the RDP server and clients. Using certificates for authentication prevents possible man-in-the-middle attacks. When a communication channel is set up between the client and the server, the authority that generates the certificates vouches that the server is authentic. As long as the client trusts the server, it is communicating with, the data being sent to and from the server is considered secure.

Contact us if any questions or concerns info@cyberclan.com