Return to the VPLS Blog

Blog Post

11 Basic Steps to Protect Your Network & Company from Ransomware

Published
Jul 28, 2021

Written by
John Headley

Filed under
Cybersecurity, Managed Security, Ransomware

Cybercrime: A Modern Plague

News articles bearing bad news that another high-profile organization is at the mercy of ransomware have proliferated since the start of the pandemic. So much so that ransomware is now considered its own "pandemic."

However, the Colonial Pipeline ransomware attack was the tipping point for the US government to act. Since that attack, several critical pieces of literature were published to help government entities and commercial organizations alike:

- Executive Order on Improving the Nation's Cybersecurity
- StopRansomware.gov

Basic Preventative Steps

Referencing the NIST Cybersecurity Framework (NISTIR 8374) that we linked above, let us review NIST's "basic preventative steps" for improving your ransomware resistance and protecting against the constant threat of compromise. Keen readers will notice a considerable overlap from our recent Ransomware Checklist blog and the preventive steps discussed in NISTIR 8374.

1. Use Antivirus Software at All Times

Set all software to scan emails and flash drives automatically.

2. Keep Computers Fully Patched

Run scheduled checks to keep everything up to date.

3. Block Access to Ransomware Sites

Use security products or services that block access to known ransomware sites.

4. Allow Only Authorized Apps

Configure operating systems or use third-party software to allow only authorized applications on computers.

5. Restrict Personally Owned Devices

On work networks, ensure only company-approved devices are connected and sharing.

6. Use Standard User Accounts

Do not use administrative accounts whenever possible.

7. Avoid Using Personal Apps

Personal email, chat, and social media should not be used from work computers.

8. Beware of Unknown Sources

Do not open files or click on links from unknown sources unless you first run an antivirus scan or look at links carefully.

9. Make an Incident Recovery Plan

Develop and implement an incident recovery plan with defined roles and strategies for decision-making. These strategies can be part of a continuity operations plan.

11. Know Your Contacts

Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement.

Ransomware Protection as a Service

These resources from the government, especially the basic preventative guidance from NISTIR 8374 that we walked through above, provide critical information that organizations should adopt as a foundation for their security program if they want to stand a chance against ransomware. However, VPLS knows that not every organization has the time, skill, or workforce to implement these cybersecurity musts.

For these organizations, VPLS can take the burden off your IT department with convenient monthly or one-time services that check all the boxes above. We have a comprehensive suite of cybersecurity service offerings, such as SOC as a Service, Managed Firewalls, Backup & DR, Managed Servers, and vCISO Services. All these services can have your organization remediating any critical cybersecurity gaps while dramatically increasing your security posture in little to no time.

Read More from this Author

John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

More from this Author

PREVIOUS
Bloom Host Game Hosting Selects VPLS as Its Col...

NEXT
VPLS Offers Comprehensive SOC-as-a-Service as P...

5 Reasons SOC-as-a-Service Features Help You

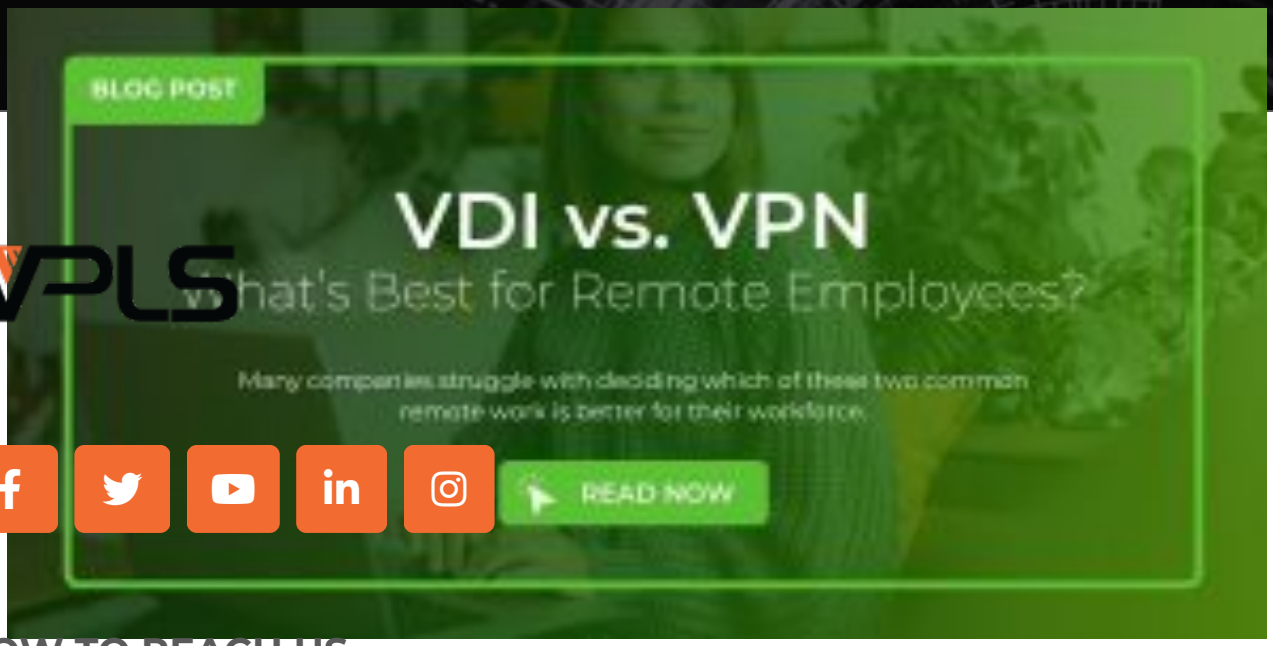
March 29, 2022

Read More »

What Is SOC-as-a-Service?

March 28, 2022

Read More »



VDI vs. VPN: What's Best for Remote Employees?

March 28, 2022

Read More »

HOW TO REACH US

Corporate Headquarters

600 West 7th Street, Suite 510
Los Angeles, CA 90017

24/7/365 Customer Service

+1 (888) 365-2656

+1 (888) 365-2656
sales@vpls.com

WHAT WE DO

Cloud
Hosting
Colocation
Network Services
Managed Services
Professional Services
VAR

WHO WE SERVE

Financial Services
Healthcare and Life Sciences
Media & Entertainment
Telecom
Startup
Enterprise
Public Sector