Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On September 16, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Palo Alto products.

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

18 September 2020

In The News This Week

Bluetooth Spoofing Bug Affects Billions of IoT Devices

The 'BLESA' flaw affects the reconnection process that occurs when a device moves back into range after losing or dropping its pairing, Purdue researchers said. A team of academic researchers have discovered a Bluetooth Low Energy (BLE) vulnerability that allows spoofing attacks that could affect the way humans and machines carry out tasks. It potentially impacts billions of Internet of Things (IoT) devices, researchers said, and remains unpatched in Android devices. The BLE Spoofing Attacks (BLESA) flaw arises from authentication issues in the process of device reconnection — an area often overlooked by security experts. Reconnections occur after two devices are connected and then one moves out of range (or disconnects) and then connects again, according to a paper published recently by researchers at Purdue University. Reconnections are common in industrial IoT environments, for example, where sensors may periodically connect to a server to transmit telemetry data, for instance, before disconnecting and going into monitoring mode. A successful BLESA attack allows bad actors to connect with a device (by getting around reconnection authentication requirements) and send spoofed data to it. In the case of IoT devices, those malicious packets can convince machines to carry out different or new behaviour. For humans, attackers could feed a device deceptive information. Read the full story here: Threatpost

Equinix data center giant hit by Netwalker Ransomware, $4.5M ransom

Data center and colocation giant Equinix has been hit with a Netwalker ransomware attack where threat actors are demanding $4.5 million for a decryptor and to prevent the release of stolen data. Equinix is a massive data center and colocation provider with over 50 locations worldwide. Customers use these data centers to colocate their equipment or to interconnect with other ISPs and network providers. Early this week, a source shared a Netwalker ransom note with BleepingComputer that was allegedly from an attack on Equinix that occurred over the Labor Day holiday weekend. This note gives us clues about how Equinix was compromised, when the attack occurred, and what data was stolen. Read the full story here: BleepingComputer

Google Play Bans Stalkerware and 'Misrepresentation'

The official app store is taking on spy- and surveillance-ware, along with apps that could be used to mount political-influence campaigns. Google is taking the step of prohibiting "stalkerware" in Google Play, along with apps that could be used in political-influence campaigns.

Effective October 1, apps that would allow someone to surreptitiously track the location or online activity of another person will be removed from the internet giant's official online store. According to Google, stalkerware is defined as "code that transmits personal information off the device without adequate notice or consent and doesn't display a persistent notification that this is happening." This includes apps that can be used to monitor texts, phone calls or browsing history; or GPS trackers specifically marketed to spy or track someone without their consent. Abusers can use such apps for the purposes of harassment, surveillance, stalking and they can even lead to domestic violence, critics say.

Google also specified that any consent-based tracking-related apps distributed on the Play Store (telemetry apps used by enterprises to keep tabs on employee activity) must comply with certain parameters. For instance, they can't market themselves as spying or secret-surveillance solutions (such as apps that go with surveillance cameras, stealth audio recorders, dash cams, nanny cams and the like). Apps also can't hide or cloak tracking behavior or attempt to mislead users about such functionality, and they have to present users with a "persistent notification and unique icon that clearly identifies the app," according to a Wednesday website notice. The new rules also include a clause meant to close down developer loopholes: "Apps and app listings on Google Play must not provide any means to activate or access functionality that violate these terms, such as linking to a non-compliant APK hosted outside Google Play." . Read the full story by Tara Seals here: Threatpost

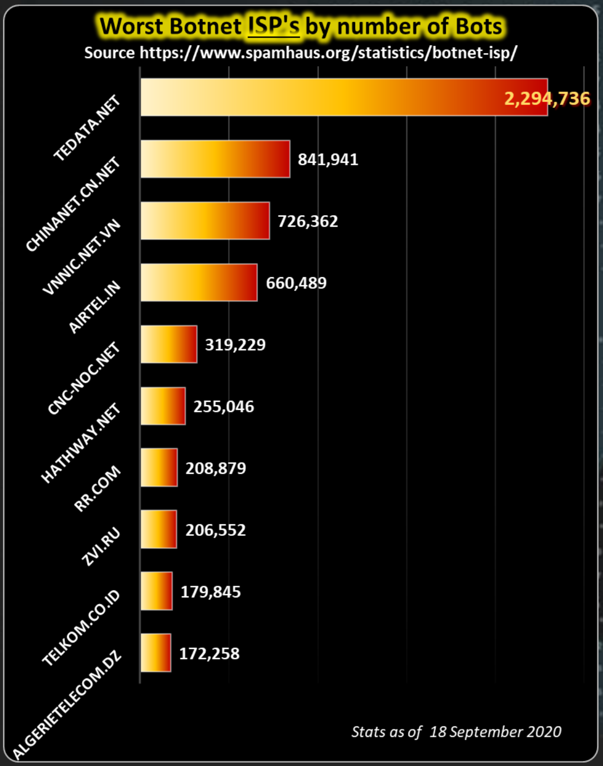
MFA Mistakes: 6 Ways to Mess Up Multifactor Authentication

This week I want to focus on common mistakes organisations make when implementing Multifactor Authentication (MFA). Normally this section is directed to individual users but this week organisations of any size are on my radar as this seems to be a common issue in various discussions I had recently. With this said, I came across this article by Joan Goodchild of Darkreading that sums it up nicely. Following is an adapted version of the article but I encourage you to read the compete article here {Darkreading.com}

Fearful of messing up its implementation, many enterprises are still holding out on MFA. Here's what they need to know.
Multifactor authentication (MFA), which requires users to authenticate their identities with at least two factors in order to access an application, appears to be gaining ground in the enterprise. A survey of 47,000 organizations conducted by LastPass late last year found 57% of businesses around the world are currently using MFA, which was up 12% over the previous year.
Statistics also make a compelling case for MFA's effectiveness. Earlier this year, Microsoft reported that 99.9% of the breached accounts it tracks didn't use MFA. Still, many businesses are holding out on implementing MFA. Too many, according Joe Diamond, vice president of product marketing at Okta. Is MFA well-used? The answer is, not to the extent that it should be," he says.
Part of the issue may be that companies still have many challenges with using it and are making implementation mistakes. MFA also can be seen as a hassle, especially for end users. And if it isn't deployed correctly, it can be as ineffective as not having any MFA in place at all. "There is a lot of work to be done to increase both the understanding and adoption of MFA," says Richard Bird, CCIO at Ping Identity.

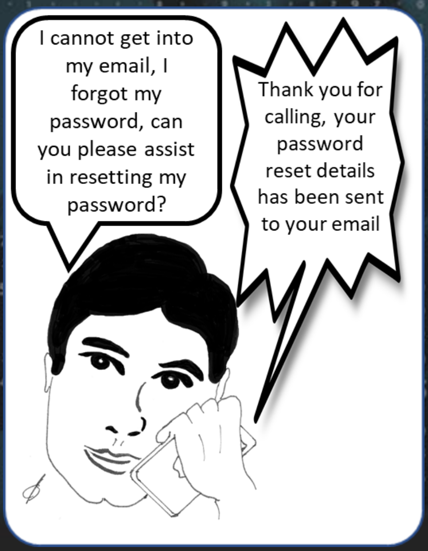
What are some of the **common missteps** organizations make when they deploy MFA? Here is half a dozen to watch out for if you're considering or using MFA for added security.

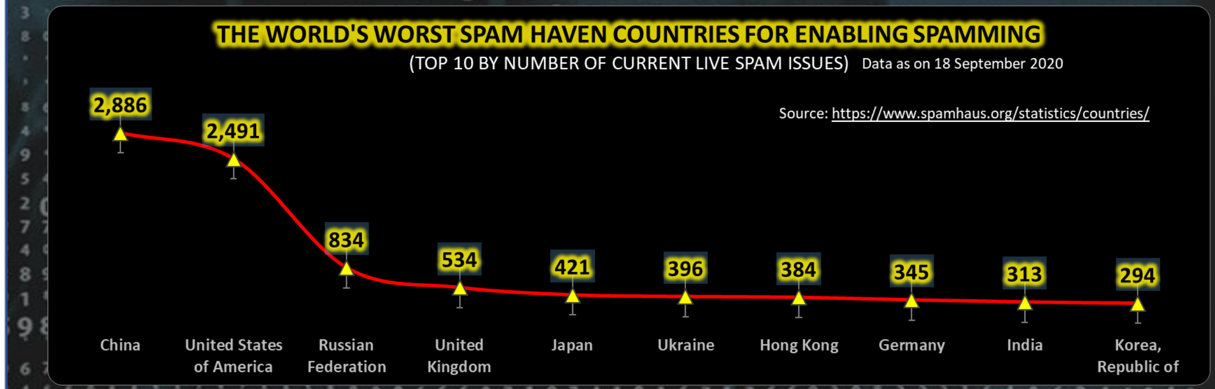
1. Allowing MFA to Be a Choice - If you're going to implement MFA, it should not be an opt-in process for end users. Ping Identity's Bird says the most common mistake he sees among customers is rolling it out as a choice or an option. "When users are given choices without a clear, value-based explanation, they will choose either the method that feels the easiest or they will stay with the method they are already comfortable with," he says. "Security is not an option. Presenting it as one is problematic." Takeaway: If you're going to implement MFA, make sure its use is mandatory.
2. Adding Friction with MFA - Using MFA as simply an extra step in security controls is a mistake, says Joseph Carson, chief security scientist and advisory CISO at Thycotic. It is important to make authentication easier through MFA, not more difficult, he says. It should be used to reduce cyber fatigue, not add to it. "While there will be some level of friction when enforcing MFA, you can minimize this by layering contextual access policies on top of the second factor," Okta's Diamond adds. Takeaway: Part of implementing MFA should be making authentication easier by removing existing poor practices.
3. Implementing MFA Only for Select Users and Apps - Deploying MFA to just some employees who are deemed critical is a common oversight that Okta's Diamond often observes among organizations. "We see organizations sometimes choose to deploy MFA just to executives because, in theory, executives have access to sensitive information," he says. "You also need to consider the other types of employees who have access to information that should not leave the confines of your organization." Stephen Banda, senior manager of security solutions at Lookout, says it is also a mistake to secure only some apps, but not all, with MFA. "We have also seen deployments where MFA is not applied to all apps that an organization uses," he says. "Again, MFA should be required for all apps because attackers can spot this vulnerability and seek to gain access with stolen credentials." Takeaway: It's best to assume all employees and apps are critical. Enforce MFA for everyone and any app that contains sensitive data.
4. Relying on SMS Alone - Using text message to authenticate is better than nothing, but doing so has a number of security issues, says Lookout's Banda. "There are two common attacks that take advantage of the SMS code authentication: mobile phishing and SIM swapping," he says. Takeaway: Instead of relying on sending an authentication code via SMS, use an authenticator app. "This will help alleviate the risk associated with the SMS code method," Banda says.
5. Deploying a Point Solution for MFA - Okta's Diamond says he often sees businesses scramble to implement MFA after a breach or an audit to address issues with authentication in one certain area, but the tools they choose meet a very narrow use case. "In the short term, these solutions seem great," he says. "However, it's eventually 'out of sight, out of mind,' and we see that the MFA solution is not properly maintained, ultimately leading to a decline in usage and once again exposing the business to the same breaches that the solution was once implemented to protect against." Takeaway: MFA implement is a holistic strategy and process. Implement MFA across the organization, and not in just one place.
6. Underestimating MFA's Impact on Business - Ping Identity's Bird says another common mistake is underestimating the impact of MFA to long-standing business processes and workflows. By nature, MFA means there will be significant changes that will impact users. These must be accounted for early in the planning process. "Changes to process flows and new demands for changes in behaviour will definitely lead to resistance to adoption," he says. Takeaway: Consider how introducing MFA will change processes for each person and each team or division and communicate those changes to users as early as possible, Okta's Diamond says. Fewer surprises will be appreciated. "Utilize your IT teams to communicate MFA deployment so that users know what to expect -- and when they need to enrol into MFA," he adds.


Worst Botnet ISP's by number of Bots
Source https://www.spamhaus.org/statistics/botnet-isp/

Stats as of 18 September 2020

For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov


I cannot get into my email, I forgot my password, can you please assist in resetting my password?
Thank you for calling, your password reset details has been sent to your email


THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES) Data as on 18 September 2020
Source: https://www.spamhaus.org/statistics/countries/

Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com