Under Pressure:
5 Corners Most IT Admins Cut (But Shouldn't)

When the pressure's on, it's tempting to cut corners. That's why we've rounded up the five most common ways IT Admins cut corners under stress, so you don't make these same mistakes.

Bad habits breed under pressure

Until the day comes that our systems achieve actual sentience, the possibility for human error will continue to pose the single greatest threat to any technology driven organization. The responsibilities of network and system administrators demand unlimited access to your most sensitive processes, and finding the balance between proper security protocols and system accessibility is an issue that every successful organization faces. Restrict access too heavily, and your team won't be able to do their jobs, but throwing open the proverbial doors will invite more than its fair share of trouble.

It is for this very reason that experienced admins who know how to navigate their systems while maintaining the best possible levels of security are worth their weight in gold, but even the best admins are capable of making mistakes when the pressure's on. Time constraints, exhaustion, and unforeseen but inevitable crises are facts of life in the modern workplace, and all of these factor into the occasional mishap. We've rounded up five of the most common mistakes that almost any admin might be embarrassed to admit they've made.

1. Poor password practices

With all the measures we take to ensure our systems' security, it's easy to take the lowly password for granted. But there isn't an easier (or more embarrassing) way to forfeit the keys to your infrastructure than typing "password123" during your initial configuration. Because the security of even the most vital systems might be thwarted by a weak password, many organizations implement password best practices and policies, which should include two-factor authentication where possible.

Unfortunately, while two-factor authentication is becoming increasingly popular with end-user applications, it's not entirely ubiquitous at the admin level. Follow proper password practices for any system you configure, even if that system's just a quick test account on your public cloud infrastructure. Sure, someone might not be able to access your hypervisor through the virtual machine, but what's to stop them from initiating a DOS attack from within your network? Weak passwords in one part of your network, even on a virtual machine, can give attackers a foothold.

It's equally important that you not use repeat passwords. Your critical systems should all be protected by unique passwords—store them in an encrypted file or application, offline if at all possible—to provide optimal protection against brute force intrusion. While these systems are likely set up to lock out repeat password attempts, lower-

priority systems like email may not be. This becomes doubly problematic because, one, if the password for the low-priority system matches that of the critical one, you've made the hacker's job that much easier, and, two, the low-priority system may actually provide an attacker the means to recover a "lost" password to the critical system.

2. Failing to Document System Changes

When a critical problem happens or something breaks, admins often try to make numerous changes very quickly to try to fix the problem. The stress of the situation and the urgency to fix the problem quickly usually means that these quick fixes are not documented. This large number of undocumented changes not only has unwanted side effects (like breaking other parts of the code) but can also cause unexpected repercussions down the road.

Nobody likes paperwork, but administrators can probably testify better than anyone just how crucial proper documentation is after the sky has come crashing down. Put simply: log everything. Every time a patch is applied, a firewall is installed, a component is configured, or a task changes hands.

Knowing a tedious task is important doesn't make it any less boring. If nothing else, it makes it that much more embarrassing when you have to admit you can't troubleshoot a critical error because you can't remember what you did to cause it. Unfortunately, this is one area where we just have to bite the bullet and fix our bad habits, though that's not to say that a good deal of documentation (e.g., access logs, firewall rule changes, etc.) can't be automated.

3. Applying patches without backing up, rebooting, or testing

Testing new software or firmware patches can take up precious time that you don't have. But the time you spend testing a patch before updating your live system may save you hours of frustration in the long run. To properly test system updates, you'll need to invest in a testing environment. This means factoring in some additional overhead in time and resources, but the investment will prove invaluable if it allows you to keep your OS or kernel up to date without sacrificing uptime, especially if that uptime means maintaining an SLA for your organization's clients or partners.

It's worth remembering that while kernel updates are likely to contain crucial fixes for security exploits, they may also pose the greatest risk to your system if your applications aren't compatible with the latest version. Schedule regular maintenance windows that both fit your organization's uptime requirements, allow ample time to back your system up, test vital updates, perform regression testing, and finally make those updates live.

And while we're on the subject of backups, it's far too easy to neglect testing those too. We tend to think of good backup systems as a "set it and forget it" process, but simply maintaining an up-to-date copy of your data may not be enough. Backups may be prone to data corruption or degradation, particularly if your system isn't configured to back up cached data. At the end of the day you're never really going to know if a backup was successfully made until you try to restore from it, and there's probably nothing more gut-wrenching than learning your backup failed after a

disaster wiped out your vital data. Schedule regular test restorations while you don't need them to save you some frustration—and maybe even your organization's future—when you do.

4. Disabling your firewall to get your application working

Firewalls protect your network in part by filtering the inbound data from the internet and either rejecting or accepting data packets based on the rules with which the firewall has been configured.

Firewalls work best when they've been properly tailored to your environment. Your firewall's rules should, for example, allow traffic based on the applications your organization is using, otherwise those applications may not have the network access they need to function. When a new application is introduced to the environment—maybe the marketing team is using a new mailing app, for example—or an application changes, however, you may be forced to make firewall configuration changes on the fly simply to allow your organization to continue to operate.

Ideally these changes should be limited, but if your phone is ringing off the hook because the sales force can't do their jobs while the firewall is hampering their CRM, disabling the firewall outright starts looking like a viable solution. Throwing open the gates to your network is never a good idea. This is another situation that's much easier to prevent with proper planning and testing than it is to troubleshoot.

5. Not turning or ignoring your IDs

It becomes second-nature: your phone goes off, you pull it out and glance over the IDS notification, and then you almost immediately dismiss it. Another false positive. Intrusion detection systems are notorious for crying wolf, and that's particularly true for systems that have not been tailored to their particular environment. You get enough false positive notifications, and it's just human nature to start ignoring them altogether. The trick is to tune your IDS in order to cut back on unnecessary notifications, depsite the fact that tuning your IDS can be both time consuming and monotonous.

Configuring an IDS properly requires days or even weeks of careful monitoring, particularly if your infrastructure includes an IPS (intrusion prevention system) that, if configured improperly, could cut the sales team's access to their customer relationship management tool or prevent clients from placing orders through your online cart. False positives are a nuisance, but false negatives can be crippling.

Allowing your IDS to run with its default configuration may feel easier in the short run, but these settings are likely to prioritize system risks that may not apply directly to your environment. This is truly an instance where a heavy investment up front can prevent a lot of heartache down the line. Once you have the historical data you need to configure it properly; prioritize IDS alert settings in the way that makes the most sense for your system in order to lend weight to the notifications you do receive and to potentially prevent malicious intrusions altogether.

Conclusion

At DigiCert, we understand the challenges that IT administrators face. Many people make compromises when they're under stress and when the pressure's high enough, even veteran administrators make mistakes they'd never want to admit to. Reducing unnecessary stress through proper planning and testing will help you to keep a cool head for those unavoidable emergencies that inevitably pop up.

Another challenge that admins are constantly dealing with is the relentless effort by hackers to devise new and ever more sophisticated exploits. It's hard enough to manage your network security without the ground always shifting under your feet, but unfortunately it's just not that easy.

That's why we've created an arsenal of powerful security tools that evolve just as fast as the everchanging security landscape. And, since SSL is often your first line of defense, we have SSL experts standing by 24/7 to help when something goes wrong. Visit our website today to learn more about securing your network from the latest threats.

Want to talk more about how CertCentral can make your SSL management simpler? Call 1.855.800.3444 or contact sales@digicert.com for further information.

digicert®