Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung
http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

This article appears in the special edition »In Depth Security – Proceedings of the DeepSec Conferences«.
Edited by Stefan Schumacher and René Pfeiffer

It's about the administrative costs

Marcus J. Ranum

Everything that's old is new again, and if you work in security long enough, you'll see the same ideas re-invented and marketed as the new new thing. Or, you see solutions in search of a problem, dusted off and re-marketed in a new niche. I'll talk about some of that, and make a few wild guesses for where this may wind up. Spoiler alert: security will not be a »solved« problem.

Citation: Ranum, M. J. (2017). It's about the administrative costs. *Magdeburger Journal zur Sicherheitsforschung*, *13*, 751–753. Retrieved May 28, 2017, from http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_050_Ranum_Costs.pdf

1 It's about the administrative costs

Computer Security's problems have mostly been a result of bad system administration. The whole regime of patch/vulnerability management that took over the industry in the early 2000s revolves entirely around the problem of applying fixes to buggy software on endpoint devices. Meanwhile, some interesting things have happened in the last decade; we see the rise of cloud computing, software as a service (SAAS), bring your own device (BYOD), and personal handsets as a substitute for desktops. The common trend-line running through all of those happenings is system administration. More exactly, it is the cost of system administration.

The most successful smartphones in the US run iOS, an operating environment that has been designed to reduce system administration costs to nearly zero. Cloud computing amortizes the cost of professionalized system administration into a one-time expense that is shared across an entire customer-base. SAAS solutions further refine the system administration cost story, removing the cost of software versioning and suite management. Put differently: the main thing that's nice about Google's gmail service is certainly not its user interface – it's that the user pays nothing to set it up and maintain it. One profound side effect of this sea-change toward aggregated system administration is that security is left in a difficult position: its role is being outsourced piece-meal in multiple directions.

Management, for over a decade, has been saying »do more with less« and »process, not people« – along with »use off-the-shelf software« and »we don't do in-house development.« Those are also implicit critiques of the cost of system administration. While computing has enabled some transformative businesses, those transformations have tended to be server-centric, residing in a data-center. The desktop, with its vulnerabilities, browsers, and malware, remains a time and money-consuming loss-leader. This is nothing new, in fact it's very old. Systems like MIT's Project Athena, and Bell Labs' Plan-9 were designed to make endpoints reliable and disposable, with near-zero incremental system administration cost. That's why cloud computing and SAAS are the current ultimate »do more with less« – they offer companies the ability to jump in and start doing things right away, and to scale in a manner that is linearly predictable. In-house development, in-house security, and occasional unpredictable desktop security breaches: those are nothing for management but an annoying bottomless downside.

The security world is about to get crushed from all sides. From the top, cloud computing Is pulling away enterprise-class responsibility, replacing it with audit and data governance. From the bottom, BYOD and portable devices threaten to obviate the desktop administration problem entirely. BYOD represents a transfer of the burden of system administration onto the user. The remaining crush, from the side, are new desktop management paradigms that may finally remove system administration as a headache. Amazingly, Microsoft has not yet reacted effectively to the threat posed by iOS-style devices as desktop replacements, but they will, eventually (typically of Microsoft: probably too late). Surprisingly, there has not yet been a general business-level ship to Apple desktops, however the new generation entering the workforce may change that. Bear in mind that Apple desktops and iOS devices are popular primarily because of the near-zero system administration load.

Computer security has put itself even more directly in the line of fire through some of its more recent practices. Standards such as PCI, and a focus on penetration testing and audit, amount to increasing the pressure on, and cost of, system administration. While audit regimes are probably the right thing to do, they're making a bad situation worse and will simply help encourage more SAAS services that remove/hide the additional cost of compliance. Security's love of compliance (which I admit I share!) amounts to putting out a fire with diesel fuel.

Unfortunately for us, »penetrate and patch« as enshrined in vulnerability management, remains the primary tool that is available for security – despite the fact that it hasn't worked in the last 20 years and isn't ever likely to. What will work is automation and professionalization of system administration, with security being folded in as a sub-specialty in release-management: the audit and governance components of security will remain but will no longer merit a large budget or role. We already see this happening in organizations where processing has moved to cloud or SAAS; security gets to review a service-level agreement to verify that the provider's paperwork includes the necessary bullet-points. There will, of course, be work for security practitioners: analysts at security-as-a-service companies, operations analysts, knowledge-builders that maintain the knowledge-bases that automate security recommendations.

Security needs to, above all, focus on its impact on and relationship to management cost. Because, in the long run, we're going to be judged on systems administrations' failures. For the system administrators, professionalizing and automating is the only way out: replace the ongoing burden of administration with a one-time cost to deploy and automate configuration management. When you read about how Google's system administration practice is so automated that administrators only pull and put systems into racks, you're seeing the future.

A standard complaint of security managers is that »security needs to learn how to talk to the business.« It's true; the business talks in terms of metrics, and computer security is hopelessly mired in fear, uncertainty, and doubt – quoting nonsense numbers like »80% of security incidents are inside jobs.« If you think about that for a minute you'll realize that such a metric is useless, and probably incorrect anyway. Security practitioners need to understand metrics, and so do system administrators. Security practitioners should look at network operations centers management measurements, or availability measurements from cloud systems administrators. If you look at that, you will notice one thing, immediately: producing such measurements requires standardized administrative practices, centralized, and highly automated. Measurable and predictable computing environments do not look like today's enterprise, with a mish-mosh of desktops running a variety of configurations, some users doing local administrative tasks and installing whatever software they like, endlessly chasing the tail of vulnerability management. The security practitioners and system administrators who come out the other side of the 2020s happily employed are going to be the ones who embrace a shift away from the 90's way of doing things; the desktop revolution is dead – long live the revolution!

2 About the Author

Marcus Ranum has been building security products and businesses since the late 1980s. He has held every job in start-ups from coder and presales support to founder and CEO, has spent thousands of hours speaking and teaching about security, and still wonders if technology will ever get any better. He writes a regular column for SearchSecurity, and blogs at the freethoughtblogs collective as »stderr«. He despises social media and politicians.