THE
ENTERPRISERS
PROJECT

A community helping CIOs and IT leaders solve problems

IT security: 4 issues to watch in 2022

What security considerations should be on the radar for CIOs and IT leaders? Keep an eye on these

By Kevin Casey

You can say this with confidence about security: It's not boring. From ransomware to initial access brokers to automated attacks to data poisoning and adversarial ML, 2021 was plenty exciting in the IT security realm.

On the brighter side, the days of security as an IT hanger-on are coming to an end, at least in larger organizations. Security ranked as the number-one IT funding priority in Red Hat's Global Tech Outlook 2021 report, with 45 percent of respondents listing it as their top funding focus.

"Security has historically often been underfunded and under-prioritized but there's

quite a bit of evidence here and elsewhere that a shift may be underway," Red Hat technology evangelist Gordon Haff said about the finding.

Paired with the growth of DevSecOps culture and practices, that becomes a powerful force for shrinking the threat landscape down to a manageable scope and improving your security readiness – which is good because the attackers and their methods don't take days off.

"Hackers won't wait for you to write a policy or procedure, ransomware won't wait for you to encrypt those databases, and script kiddies won't wait for your next patch management cycle before they launch their latest exploit," says Aladdin Elston, head of information security at Altimetrik.

With that in mind, it's time to take stock and refocus on security goals for IT teams and their larger organizations. Here are four considerations to keep in mind for 2022.

[Want a shareable primer on DevSecOps and its benefits? See What is DevSecOps?]

1. Double back to the basics (again)

If infosec had a greatest hits album, basic security hygiene would be track one. Year in, year out, the root cause of many security incidents can be traced back to the fundamentals. A wide range of threats, from ransomware to cloud account hijacking to data leakage, owe much of their efficacy to surprisingly simple missteps, from a misconfigured setting (or even a default setting left unchanged) to an over-privileged user to unpatched software.

"In 2022, you may think that the basics should already be covered," Elston says. "However, many of the most basic security practices aren't followed and can lead to massive breaches."

[Need a DevSecOps primer? Read How to explain DevSecOps in plain English.]

This begs the question: What are the basics? Things like password hygiene and system patching apply across the board, but you also need to identify and agree with colleagues on "the basics" required in your specific organization. That gives you a collective standard to work toward and measure against. Moreover, the word "basic" doesn't do some of the fundamentals justice.

doesn't do some of the fundamentals justice

"In my world, the basics are patch management, secure configuration, threat modeling, DAST and SAST scanning, internal and external vulnerability scanning, penetration testing, defense against phishing attacks, third-party vulnerability assessments, backup and disaster recovery, and bespoke security training," Elston says.

There are many worthwhile security tools and technologies, and they're as necessary as ever – especially those that enable security automation. A "we have all the tools" mindset can lead people to ignore core security needs or simply assume they're taken care of, however.

"Basic" doesn't mean old, either. SAST and DAST scans are key methods in the DevSecOps lifecycle, for example – part of the practical implementation of the popular "shift left" mantra.

[Related read: How to create an effective security policy: 6 tips.]

2. You can't prioritize everything

Consider (re)doing a gap analysis in your organization as part of a back-to-basics program, especially if you haven't completed one lately. Elston points to a slew of external frameworks that you can use, such as NIST Cyber Security Framework, OWASP Top 10, and others. MITRE ATT&CK is another to consider. Regulatory rules (like HIPAA or PCI) apply where relevant. Cloud-centric shops, also check out Red Hat's whitepaper, "A layered approach to container and Kubernetes security."

Elston recommends starting with an inventory check of all assets. You can't test or protect what you aren't aware of – your inventory becomes the basis for both internal and external vulnerability assessments, as well as internal and external pen testing, among other proactive security strategies.

This is a point at which people and organizations sometimes get lost in the threat landscape. The list of risks and vulnerabilities you discover in your company, especially when you dig into those external frameworks or other resources that cover known threats and CVEs, can seem infinite. You need to shrink things down to size. If you try to address everything, you risk protecting nothing, particularly given that the potential threats increase year after year.

"You will likely end up with a list of your greatest risks to the organization, which you can then rank and prioritize in order of criticality and organizational importance," Elston says. "I would start by focusing on the top 20 percent in that ranked list."

This approach offers two primary benefits. First, focusing on your most urgent risks is both efficient and results-oriented. It's a way of taking broad security wisdom and making it specific and actionable in your organization. Moreover, it makes a massive effort – an applicable description for security – manageable for people.

Second, it can actually have a downstream effect because in focusing on the most severe vulnerabilities, you begin to identify patterns that become repeatable elsewhere.

> If you try to address everything, you risk protecting nothing, particularly given that the potential threats increase year after year.

"More often than not, the most critical vulnerabilities will offer insight about your environment, your network, and your people," Elston says. "In the process of identifying where the weaknesses are and how to correct them, you'll develop a cadence of approach that can be applied to lower-priority issues."

Elston also stresses the importance of building an internal channel for different people and teams to communicate on and collaborate on security issues. This is something you can (and should) do if you're not all-in on the DevSecOps approach.

"Thankfully, with responsible disclosure programs, crowd sources, and penetration testing, many vulnerabilities can be identified early and patched quickly," Elston says. "This makes it essential to have a clear and positive communication channel setup within your IT, infrastructure, security, and development teams."

3. Supply chain issues, meet IT security

The shipping and logistics metaphor used to characterize cloud-native application development – think containers, microservices, and orchestration – is also relevant in the context of our recent obsession with global supply chains. The details are different, but many of the principles of supply chain management – and especially supply chain security – have become highly applicable in IT.

“Supply chain is a hot topic *everywhere*,” Haff from Red Hat tells us. “And that includes software, including open source software.”

How hot? Enough so that The White House issued an executive order on cybersecurity in May 2021.

Just like in other supply chains, most software depends *on other software* to get built, packaged, and deployed. Even organizations with massive development teams use code that they didn’t write from scratch – often lots of it.

“Most software that organizations write depend on software obtained from elsewhere – including software downloaded from the internet,” Haff says. “Most of the code isn’t malicious, but like all software, it may contain bugs or may simply be an old version.”

Software supply chains are critical areas for IT security in 2022 and beyond. In fact, one way to think about DevSecOps is that it fundamentally focuses on security as a supply chain paradigm rather than, say, a network perimeter issue. This is why trusted container registries (like Quay) and automated image scans are increasingly important, too.

Haff notes that industry groups like the Open Source Security Foundation (OpenSSF) are already tackling supply chain issues at the macro level. But IT pros will need to bring this mindset to their own organizations, too.

> Software supply chains are critical areas for IT security in 2022 and beyond.

“IT managers need to do their part by developing an awareness of the problem and making the best use of software scanning and signing tools to mitigate it as part of their DevSecOps workflows,” Haff says.

Kirsten Newcomer, director, cloud and DevSecOps strategy, Red Hat, expects supply chain security to be a huge focal point for IT leaders and their teams in 2022. Organizations will recognize that existing methods such vulnerability analysis alone won’t be sufficient to protect against potential intrusions. DevSecOps teams will expand their strategies and toolchains in an effort to protect the supply chain itself.

“To do this, we’ll see investments in adopting new technologies in pipelines, such

as Tekton CD chains as well as Sigstore, to make it easier to add signing in the pipeline," Newcomer says.

In fact, Newcomer sees another manufacturing and supply chain metaphor arising in IT: the software bill of materials (SBOM).

"Proposed standards around delivering SBOMs have been around for quite some time, but because of concerns around supply chain security, we've reached the point where all organizations are going to need to figure out how to deliver a software bill of materials," Newcomer says, adding that there will be discussion and debate in the industry about static and dynamic BOMs.

The latter would include evolving information such as vulnerability data: The software package itself hasn't changed, but known vulnerabilities associated with that package have.

"Related to this, automation around SBOMs and related package metadata is going to explode," Newcomer says.

4. It's all about the data

Traditional areas of concern like endpoint and network security still matter. But security – for both malicious actors and the people and organizations trying to stop them – boils down to data, much of it distributed across multiple environments. All of the buzzword-y business expressions like "data is the new currency" and the like? Cybercriminals subscribe to that idea.

Cloud security is a huge topic not because cloud infrastructure is less secure. It's a huge topic because virtually everyone has a cloud footprint now – and that's often where the data is.

Organizations should prioritize tools and strategies such as role-based access control and zero trust or they will leave themselves open to unnecessary risks, says Gal Diskin, CTO and co-founder of Authomize. Diskin advises continuously optimizing everything under your identity and access management umbrella. The "assume you've been breached" mindset applies: Assume your cloud accounts, from infrastructure to SaaS and beyond, will be breached at some point.

"You should expect business accounts to be compromised and plan your security strategy accordingly," Diskin says, "Defend in depth and use tools that can help limit

the blast radius of account compromises. Make sure you continuously validate access, not just at the coarse authentication layer but also at the granular authorization level."

[Related read: What is ransomware? 5 facts IT leaders should understand now.]

Melinda Watts, head of global services at ZL Technologies, expects that security teams that have been focused on infrastructure in the past will increase their attention to the data that resides in or travels through that infrastructure in the year ahead.

Specifically, Watts predicts that organizations will pay more attention to their dark data from a security perspective. In layperson's terms, dark data refers to the copious amounts of information that organizations produce and store but don't really do anything with.

More on DevSecOps

- **Cheat Sheet: DevOps Glossary**
- **What is DevSecOps?**
- **How to explain DevSecOps in plain English**
- **5 DevSecOps open source projects to know**
- **Guide: A layered approach to container and Kubernetes security**
- **DevSecOps pipelines and tools: What you need to know**

"DevSecOps have long taken a top-down approach to security, ensuring that the storage infrastructure – cloud or on-premises – is secure," Watts says. "However, in 2022 we will see this work supplemented by a bottom-up approach, in which enterprises will take newfound focus on the security of the data stored within these systems."

Some organizations already have that balance, but those that have prioritized infrastructure over data in the past will be working hard to catch up. Attackers don't brag about the server they compromised – they get excited about the data they find on it, or elsewhere in an organization once they use that server (or container or sign-in credential or, well, you get the picture) as an open door.

This is why ransomware has become a monster business and will continue to be a blight, especially in high-profile sectors like healthcare, banking and financial services, and government.

“Health data security has been an emerging trend for years, and it will start to get significant attention with the continued occurrence of ransomware attacks in the years to come,” Elston says.

[How do containers and Kubernetes help manage risk? Read also: A layered approach to container and Kubernetes security.]

Kevin Casey writes about technology and business for a variety of publications. He won an Azbee Award, given by the American Society of Business Publication Editors, for his InformationWeek.com story, "Are You Too Old For IT?" He's a former community choice honoree in the Small Business Influencer Awards.

More about me ›