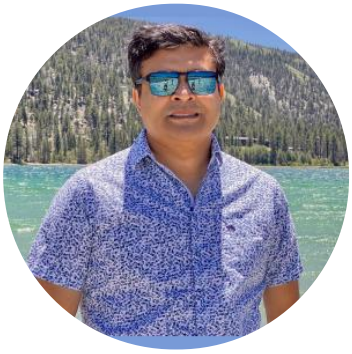
SHOW NOTES

@mjkabir Notes



https://shownotes.app/show/s71bq

Infrastructure Security for Startups

Launching a public website or app is a must for all tech startups. Some startups are software companies, so they should know what software/services they need to keep their infrastructure safe and secure.

I will share some pointers that might help you if you are unsure how to enhance your security on a small budget. Expect to spend 5-15% of revenue for on going security.

TABLE OF CONTENTS

Perform Penetration Tests

There are lots of pen-testing vendors. I have some personal biases that I should disclose:

I usually avoid a company that does not disclose its pricing. These companies usually require you to sign up for a "DEMO," if they want to coach you into a high-price service plan. But not all of them are bad. Some of them are probably extraordinary, and I am missing them. No regrets so far. But if this bugs you, please ask for a DEMO and enjoy wasting your valuable time with a "sales engineer" :)

I recommend:
Pentest-Tools.com
Immuniweb.com

422 days 18 hrs ago

Log Everything!

Log everything and keep copies of all logs off-site. Here are some great third-party log service solutions.

Paid Services (Low Cost to High):

- **Loggly** (by SolarWinds)
- **Papertrail** (by SolarWinds)
- **Sumo Logic**
- **Logz.io**
- **Datadog**
- **New Relic**

Open Source Services (Hosted and On-Premise):

1. **Graylog**
2. **Elastic Stack (ELK Stack)**
3. **Fluentd**
4. **Prometheus** (with logging add-ons)
5. **Loki (by Grafana)**

423 days 4 hrs ago

Deploy Web Application Firewall (WAF)

I recommend ModSecurity, an open-source, cross-platform web application firewall (WAF) module. Known as the “Swiss Army Knife” of WAFs, it enables web application defenders to gain visibility into HTTP(S) traffic. It provides a power rules language and API to implement advanced protections.

Of course, if you prefer to pay for your WAF solution, there are plenty of companies that will take your money.

1. **Cloudflare WAF is** easy to set up, scales with traffic, is affordable for startups (a free tier is available), has built-in DDoS protection, and offers automatic updates. It is best for Startups looking for a comprehensive, easy-to-deploy solution that also provides CDN functionality.

2. **AWS WAF** offers native integration with AWS services, pay-as-you-go pricing, easy integration with Amazon CloudFront, and AWS Application Load Balancer. It is best for Startups already using AWS infrastructure who want seamless integration with their existing setup.

3. **Azure WAF** offers native integration with Microsoft Azure, automatic threat detection, and easy scaling with Azure resources. It is best for Startups leveraging Microsoft Azure infrastructure.

4. I**mperva Cloud WAF** offers robust security features, including DDoS protection, good reporting and analytics, and flexible configuration. It is best for Startups seeking robust protection against web attacks with minimal configuration effort.

5. **F5 Advanced WAF** offers both hardware and virtual appliances. It offers advanced security capabilities, including protection against sophisticated bots, API protection, and application-layer DDoS mitigation. It is best for Startups with more complex infrastructure that need fine-tuned control over WAF policies.

6. **Barracuda WAF** offers Cloud, hardware, or virtual appliances. It is easy to deploy, offers strong protection against OWASP's Top 10 vulnerabilities, and integrates well with on-premise and cloud infrastructure. It is best for Startups with hybrid or on-premise infrastructure needs.

423 days 4 hrs ago

Create a Bug Bounty Program

This is not a cheap option, as most Bug Bounty management platforms are expensive.
For early-stage startups with limited budgets, the following are good bounty programs:

1. Open Bug Bounty: This non-profit platform allows researchers to report vulnerabilities and offers a free, non-monetary reward system. You can set up a free account without any financial commitment.
2. Bugv: Bugv offers a pay-per-report pricing model, which could be more manageable for small startups. It also provides additional features like disclosure assistance and report validation.
3. BountyGraph: This platform supports monetary and non-monetary rewards (e.g., swag, points, or recognition). Pricing starts at $99/month and offers an affordable pay-per-report option.
4. Hacktivity: A community-driven platform that allows researchers to submit vulnerabilities on various websites. It's free to set up an account and receive vulnerability submissions.
5. CrowdSecurity: This community-driven platform coordinates vulnerability and bug bounty programs and offers different pricing plans starting at €50/month.

Among these, my favorite is the Open Bug Bounty platform. For early-stage or solo startup founders with limited budgets, Open Bug Bounty offers a compelling platform. Here's how it can work for them:

Free Bug Bounty Program: Startups can launch a bug bounty program at no cost. This allows access to a wide pool of security researchers without needing upfront payments.

Non-Profit Structure: The platform operates as a non-profit, designed to benefit website owners and researchers without commercial interests. Startups can utilize it to secure their platforms without worrying about expensive fees.

Flexible Gratitude System: Founders are not obligated to pay researchers. They can express appreciation non-monetary, such as a thank-you message or small gifts, making it ideal for startups with tight financial constraints.

Ethical and Non-Intrusive Testing: The platform ensures that all vulnerabilities are reported ethically, using non-intrusive methods that won't harm a startup's infrastructure.

In short, the platform provides startups an affordable way to secure their websites through crowdsourced vulnerability testing while maintaining complete control over researcher interactions and financial rewards.

Open Bug Bounty for Website Owners

For funded startups, several bug bounty platforms can help identify vulnerabilities and secure your software:

1. Bugcrowd: Through its CrowdControl platform, Bugcrowd offers a comprehensive suite of vulnerability coordination and bug bounty program management tools. It caters to startups and has a diverse community of researchers.
2. HackerOne: This platform connects users with a global community of ethical hackers. It offers a managed service option and features such as vulnerability disclosure programs, penetration testing, and more.
3. Synack provides an AI-enabled platform with a curated community of ethical hackers. It is suitable for startups looking for targeted testing and managed services.
4. Intigriti: A European-based platform that offers tailored bug bounty programs for businesses of all sizes. Provides access to a curated community of ethical hackers.
5. YesWeHack: A global bug bounty platform that offers public and private programs, vulnerability disclosure policies, and a diverse community of researchers. Suitable for startups looking for an easy-to-use platform.

423 days 4 hrs ago

Prepare for SOC 2 Readiness

SOC 2 (System and Organization Controls 2) is an auditing standard created by the American Institute of Certified Public Accountants (AICPA) to assess how companies handle and protect customer data. It's especially important for service providers, such as SaaS companies, that store or process information on behalf of customers.

SOC 2 focuses on five key Trust Service Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. These criteria ensure systems are designed to safeguard customer data and operate securely and reliably.

There are two types of SOC 2 reports:

- **Type I**: Evaluates the design of controls at a specific point in time.
- **Type II**: Assesses the operational effectiveness of controls over a period (usually 6-12 months).

Achieving SOC 2 compliance demonstrates to customers and partners that your organization follows industry best practices for data security and privacy.

How a Small Startup Can Achieve SOC 2 Compliance

Achieving SOC 2 compliance may seem daunting for a small startup, but breaking it down into manageable steps can make it more feasible. Here's how to go about it:

1. **Understand SOC 2 Requirements:** SOC 2 focuses on five Trust Service Criteria:
    - **Security**: Protecting systems from unauthorized access.
    - **Availability**: Ensuring systems are operational as agreed.
    - **Processing Integrity**: Data processing is accurate and authorized.
    - **Confidentiality**: Sensitive information is protected.
    - **Privacy**: Personal data is handled properly and safeguarded.
2. **Perform a Gap Analysis:** Evaluate your current processes and identify gaps in security controls. Focus on areas like access control, risk management, monitoring, and incident response.
3. **Implement Security Controls:** Once gaps are identified, start implementing required controls:
    - Ensure strong access control policies are in place.
    - Log and monitor system activities for suspicious behavior.
    - Encrypt sensitive data at rest and in transit.
    - Establish an incident response plan.
4. **Hire or Consult SOC 2 Experts:** Work with consultants or automated SOC 2 platforms (e.g., Drata, Vanta) to guide you through compliance. They can help streamline

documentation and implementation.

5. **Prepare for the Audit:** Conduct a readiness assessment to ensure your controls are working properly before the official audit. Make sure documentation and evidence are ready.
6. **Choose Type I or Type II Audit:**
   - **Type I**: Focuses on the design of controls at a specific point in time. It's quicker and easier to achieve.
   - **Type II**: Assesses the operational effectiveness of controls over a period (usually 6-12 months). It's more in-depth and required for long-term compliance.
7. **Select an Audit Firm:** Hire a licensed CPA firm that specializes in SOC 2 audits. Make sure they are experienced in working with startups.
8. **Maintain Compliance:** SOC 2 compliance is an ongoing process. Regularly review and update your security policies to stay compliant over time.

Following these steps will help you navigate SOC 2 compliance as a small startup, ensuring your platform meets industry security standards and builds trust with customers.

423 days 4 hrs ago

Must Have Offsite Backups

I love rsync.net for simple and cost-effective off-site backup for servers.
For desktops and laptops, I prefer Carbonite.
423 days 2 hrs ago

Have White Hat Hackers on Speed Dial

Security incidents happen at the oddest moments. Having professional white hat hacker(s) on speed dial is a blessing. Have a well-defined protocol for communicating the severity of your needs to the security experts so you can tap into them when needed.

For example, an organization can access two or three levels of white hats with different degrees of commitment for on-call duties. By establishing a well-defined communication protocol, you can convey the severity and urgency of your security needs quickly and effectively.

422 days 18 hrs ago