When Serverless Met Security...
Serverless Security & Functions-as-a-Service

Niels Tanis - CA Veracode
About me

• Niels Tanis
  • Security Researcher
  • Background in:
    • .NET development
    • Pen tester
    • Security Consultancy
    • CSSLP
SERVERLESS ECONOMIC IMPACT

Daniel Stori {turnoff.us}
Agenda

• Serverless Security - Functions-as-a-Service (FaaS)
  • Overview
  • Benefits
  • Downsides
• Conclusion
• Q&A
What is Serverless?

• Full abstraction of servers
• Instant, scalable and event-driven
• Pay-per-use
• ‘Cloud is an operating system Serverless is its native code!’ (Erik Peterson, QCON)
Functions-as-a-Service (FaaS)

- FaaS != Serverless
- FaaS is key building block
- Stateless & Ephemeral
- Single Responsibility
- Scalable & Event driven
Example Waste Management System

Security benefits of Serverless

• Servers are maintained by vendor
• No server to be compromised?
  • ‘Gone in 60 Milliseconds’ - Rich Jones
• Denial of Service is mitigated?
Denial-of-Service

- Network DoS mitigated
- What get’s executed? Let’s limit it!
- Denial-of-Service Wallet
Attack Surface

• App shattered across platform
• Lot of complexity
• Inner- and outer attack surface
Monitoring

• What has happened?
• Logging and correlation
• What are you monitoring/logging
Developed Code == Vulnerabilities

• Developed in various languages/technologies
• Old ‘fashioned’ vulnerabilities
  • SQL Injection
  • Remote Code Execution
  • Log Injection
Third Party Libraries

• Simple Azure Function in C# - 10 lines
  • 50k lines for Azure Functions Host
  • 120k lines for Newtonsoft.JSON
• Vulnerability found/published
• Malicious/compromised package
Storing Secrets

- Environment variables
- Use platform vendor service
- ‘Secrets at Scale’ - Ian Haken of Netflix
Encryption of data

- Protecting data in transit and at rest
- Most vendors do ‘transparent’ encryption for data at rest.
- Consider ‘Client-Side Encryption’ in transit
Least Privilege

- Fit for purpose privileges
- Review or audit them over time
Software Supply Chain

- Automation is king!
- Deployment as code
- Separate different environments
  - Development
  - Staging
  - Production
Conclusion

• Easy to create! Hard to keep track!
• Threat modelling
• Compartmentalise
• Monitoring and logging
• Automate delivery and configuration
Thanks! Questions?

- ntanis at veracode.com
- https://twitter.com/nielstanis
Links

- Serverless Security and Things That Go Bump the Night - [https://www.infoq.com/presentations/serverless-security](https://www.infoq.com/presentations/serverless-security)
- Storing Secrets at Scale - [https://www.youtube.com/watch?v=15H5uCj1hlE](https://www.youtube.com/watch?v=15H5uCj1hlE)
- Gone in 60ms - [https://www.youtube.com/watch?v=YZ058hmLuv0](https://www.youtube.com/watch?v=YZ058hmLuv0)