ONAPSIS

WE SECURE BUSINESS CRITICAL APPLICATIONS. WE SECURE BUSINESS.

FIVE THINGS EVERY LEADER AND ORGANIZATION SHOULD BE DOING TO SECURE SAP

KYLE RAMSEY

STRATEGIC ACCOUNT MANAGER – EASTERN CANADA

AGENDA

01. History Of Onapsis

02. State Of SAP Security

03. Five Things Every Leader And Organization Should Be Doing To Secure SAP

ONAPSIS

HISTORY OF ONAPSIS

History Of Onapsis

- 2000-2009: CEO, CTO, and CIO were former pen-testers and found a lot of easy ways to hack into SAP
- 2009-2016: The trio created a software, which started with application / system / “Basis” and HANA database-layer ad-hoc vulnerability management, grew into ITGC testing and validation, then evolved into real-time threat detection and response
- 2018: Released threat report with intelligence firm Digital Shadows which discovered several SAP exploits and increased attacks and malicious activity surrounding SAP across the dark web, hacker forums, social media, and paste sites
- 2019: Acquired Virtual Forge, who were the experts on the code and transport layers, becoming the one stop shop for SAP security at the four main layers: application, database, code, and transports
- 2019: Discovered 10.0 CVSS v3.1 exploit was publicly available on GitHub (researcher from ERPScan; Russian company banned by the U.S. Treasury) and led proactive efforts to help customers protect themselves
- 2023: The only cybersecurity and compliance solution for SAP, endorsed by SAP
- To date: Six United States Department of Homeland Security CERT (Computer Emergency Readiness Team) Alerts have been yielded through Onapsis’ research
- To date: Onapsis Research Labs has discovered 700 + zero-day vulnerabilities in SAP

STATE OF SAP SECURITY

State Of SAP Security

- 2021: Observed through honeypot technology that hackers are:
  - Exploiting SAP systems less than 72 hours after Patch Tuesday
  - Patching SAP systems to cover their tracks
  - Conducted over 300 successful in the wild SAP exploitations throughout the study
- 2022: Research helped yield over 40 SAP security notes
- March 2023: Three of the six HotNews notes were attributed by Onapsis, all four High Priority notes were attributed by Onapsis
- Exploits are now 50 + and continuing to proliferate
- Ransomware as a Service, ChatGPT
- SaaS applications such as SuccessFactors have advanced, granular vulnerabilities as well such as logging settings, user impersonation, and configurations that traditional vulnerability management tools cannot scan for
- Despite shift to cloud, SaaS, and managed services, you of course have and always will own your data

FIVE THINGS EVERY LEADER AND ORGANIZATION SHOULD BE DOING TO SECURE SAP

Five Things Every Leader And Organization Should Be Doing To Secure SAP

- 1. Gain visibility with one tool (transition from several tools, spreadsheets, and screenshots, and reports, to one, single, consolidated GUI and dashboard that integrates with the ecosystem of your other tools)
- 2. Keep up not only on patches, but also misconfigurations, parameters, SODs, and authorizations (manual steps are often omitted… threat actors are leveraging unpatched vulnerabilities in less than 72 hours)
- 3. Detect and respond in real-time (need to be alerted on a 24/7 basis if threat actors are attempting to exploit vulnerabilities… also need compensating controls around backlog of patches… whether that's due to volume or fear of downtime… strive to no longer "accept risk"… the undetected fraud may have already been committed or is being committed as we speak… operational disruption may have already occurred or is occurring as we speak)
- 4. Secure code and transports (not just ABAP, but also other languages such as Javascript and SAPUI5 Fiori)
- 5. Build a governance model and report on risk reduction cross-functionally (not just SAP teams, but cybersecurity and audit teams as well)
- 6. Overcommunicate! SAP security ownership has historically been a hot potato… as an organization, overcommunicate on what the program is and own it!

THANK YOU! Q&A