OVERVIEW OF SOFTWARE SECURITY BEST PRACTICES

Richard Greenberg, CISSP
CEO/CISO Security Advisors LLC
ISSA Hall of Fame
Former OWASP Global Bd of Directors

RICHARD GREENBERG

- CEO/CISO, SECURITY ADVISORS LLC
- CEO LAYER 8 MASTERS
- ISSA INTERNATIONAL HALL OF FAME, HONOR ROLL AND DISTINGUISHED FELLOW
- FORMER OWASP GLOBAL BOARD OF DIRECTORS
- PRESIDENT, ISSA LOS ANGELES
- FORMER PRESIDENT, OWASP LOS ANGELES
- FOUNDER & CHAIR, WOMEN IN SECURITY FORUM

A HUGE PART OF SOFTWARE VULNERABILITIES IS NOT TECHNICAL

- THROWING MORE MONEY AND TOOLS ONLY AT THE PROBLEM WILL NOT WORK
- NEED A WELL DEFINED FRAMEWORK
- NEED A STRATEGY AND PLAN, INCORPORATING MANY AREAS OF THE BUSINESS (INFOSEC, DEVELOPMENT, PROJECT MGMT, OPERATIONS, CLOUD)
- ORGANIZATIONS MUST DELIVER BETTER SOFTWARE WITH FEWER SECURITY FLAWS

CURRENT STATE OF APPLICATION SECURITY

- 98% OF WEB APPLICATIONS ARE VULNERABLE TO ATTACKS THAT CAN RESULT IN MALWARE, REDIRECTION TO MALICIOUS WEBSITES, AND MORE. *
- 58 OF THE 103 BIGGEST INCIDENTS OF THE LAST 5 YEARS (56%) TIE BACK TO SOME FORM OF WEB APPLICATION SECURITY ISSUE **
  - Marriott International data breach (2018)
  - First American Financial Corporation data leak (2019)
  - Yahoo data breach (2013-2016)
  - Equifax breach (2017)
  - Facebook data exposure (2019)
  - LinkedIn data breach (2021)
- 74% OF CODEBASES CONTAIN HIGH-RISK OPEN SOURCE VULNERABILITIES***

* SOURCE: PT SECURITY

** CYENTIA, THE STATE OF THE STATE OF APPLICATION EXPLOITS IN SECURITY INCIDENTS

*** SYNOPSYS OPEN SOURCE SECURITY AND RISK ANALYSIS (OSSRA) REPORT

CURRENT STATE OF APPLICATION SECURITY

- WEB APPLICATION BREACHES ACCOUNT FOR 25% OF ALL BREACHES *
- 91% OF CODEBASES CONTAIN COMPONENTS 10 OR MORE VERSIONS BEHIND**
- MAJORITY OF SECURITY FLAWS ARE FOUND NOT BECAUSE THEY DIDN'T EXIST YESTERDAY, BUT BECAUSE WE HAVE IMPROVED OUR ABILITY TO DETECT THEM
- MOST FLAWS IDENTIFIED YEARS AGO BUT KEEP SHOWING UP
  - SQL Injection: in the OWASP Top 10 in 2007 and is still there!
- ORGANIZATIONS NEED TO CHANGE THE WAY THEY ARE DEVELOPING SOFTWARE

* VARONIS 2024 DATA BREACH REPORT

** SYNOPSYS OPEN SOURCE SECURITY AND RISK ANALYSIS" (OSSRA) REPORT.

BUILD TIES WITH THE APP DEVELOPMENT TEAM

- ESTABLISH AND CULTIVATE A CLOSE RELATIONSHIP WITH THE HEAD OF APPLICATION DEVELOPMENT
- COMPANIES NEED TO SHIFT LEFT TO BAKE SECURITY INTO THE SDLC
- UNDERSTAND THAT UNIVERSITIES ARE STILL FAILING AT HAVING ENOUGH INFOSEC IN THE CURRICULUM FOR APP DEVELOPERS
- LOOK FOR DEVELOPERS WHO WANT TO BE ENGAGED WITH SECURITY
- CREATE "SECURITY CHAMPIONS" TO BRIDGE THE GAP WITH DEVELOPMENT
- HAVE ALL STAFF IN APPDEV TAKE SECURE CODING TRAINING
- MEET WITH APP DEV TEAM REGULARLY

BAKE SECURITY INTO THE SDLC

- UTILIZE STATIC/DYNAMIC/INTERACTIVE APPLICATION SECURITY TESTING
  - There are several open source solutions available, such as Zed Attack Proxy (ZAP)
- USE SOFTWARE COMPOSITION ANALYSIS (SCA) TOOLS
  - SCA from OWASP: Dependency Check and Dependency Track
- AUTOMATE AS MUCH AS YOU CAN
- HIRE A PENETRATION TESTER FOR CRITICAL APPS

INTEGRATE THREAT MODELING INTO THE SDLC

- IMPORTANT TO ADOPT A SYSTEMATIC APPROACH TO IDENTIFY AND ADDRESS POTENTIAL THREATS EARLY
- DONE PRIOR TO ANY CODE REVIEW
- KEEP AN UP-TO-DATE INVENTORY OF THREAT MODELS
- PRIORITIZE THE THREATS
- BUILD A TEAM TO DO THE MODELING, INCLUDING BUSINESS ANALYST, SECURITY, AND DEVELOPER
- USE EXISTING DEVELOPMENT WORKFLOW TOOLS FOR THREAT MODELING WORKFLOW

WEB APPLICATION FIREWALLS

- CAN HELP COVER UP A MULTITUDE OF CODING SINS
- OFTENTIMES DEPLOYED TO JUST DETECT AND BLOCK OWASP TOP 10 ATTACKS
- CAN BE CHALLENGING TO PROPERLY CONFIGURE
- EASY TO GET TOO MANY WAF ALERTS OR FALSE POSITIVES
- ORGANIZATIONS GET COMPLACENT AND THINK THE WAF COMPENSATES FOR POOR CODING
- IN DEVOPS ENVIRONMENTS, IT CAN BE CHALLENGING KEEPING WAF UP-TO-DATE WITH SOFTWARE CHANGES
- LOOK FOR NEWER WAFS THAT PROVIDE API PROTECTIONS AND CLIENT-SIDE ATTACK PREVENTION

FAMILIARIZE YOURSELF WITH OWASP

- OWASP IS A GLOBAL COMMUNITY THAT DRIVES THE VISIBILITY AND EVOLUTION IN THE SAFETY AND SECURITY OF THE WORLD'S SOFTWARE
- EVERYONE IS FREE TO PARTICIPATE IN OWASP AND ALL OF OUR MATERIALS ARE AVAILABLE UNDER A FREE AND OPEN SOFTWARE LICENSE
- OWASP IS A REGISTERED NONPROFIT IN THE UNITED STATES AND EUROPE, SO ALL OF YOUR FINANCIAL CONTRIBUTIONS ARE TAX DEDUCTIBLE

OWASP CORE VALUES

- **OPEN**

  EVERYTHING AT OWASP IS RADICALLY TRANSPARENT FROM OUR FINANCES TO OUR CODE

- **INNOVATION**

  OWASP ENCOURAGES AND SUPPORTS INNOVATION AND EXPERIMENTS FOR SOLUTIONS TO SOFTWARE SECURITY CHALLENGES

- **GLOBAL**

  ANYONE AROUND THE WORLD IS ENCOURAGED TO PARTICIPATE IN THE OWASP COMMUNITY

- **INTEGRITY**

  OWASP IS AN HONEST AND TRUTHFUL, VENDOR NEUTRAL, GLOBAL COMMUNITY

OWASP GUIDANCE

- RISKS: OWASP TOP TEN, MANDATED BY PAYMENT CARD INDUSTRY (VISA, AMEX, MASTERCARD) ARE THE MOST CRITICAL SECURITY RISKS TO WEB APPLICATIONS
- STANDARDS: APPLICATION SECURITY VERIFICATION STANDARD (ASVS) PROVIDES A FRAMEWORK FOR TESTING WEB APPLICATION TECHNICAL SECURITY CONTROLS
- CHEAT SHEETS: A SET OF SIMPLE GOOD PRACTICE GUIDES FOR APPLICATION DEVELOPERS AND SECURITY TEAMS (OVER 60)
  - Docker Security Cheat Sheet
  - Threat Modeling Cheat sheet
  - Kubernetes Security Cheat Sheet

OWASP GUIDANCE (CONT'D)

- CHECKLISTS: MOBILE APPS CHECKLIST, WEB APPLICATION SECURITY TESTING CHECKLIST, TESTING METHODOLOGY CHECKLIST, SECURE CODING PRACTICES QUICK REFERENCE GUIDE
- TEST GUIDES: THE MOBILE SECURITY TESTING GUIDE (MSTG) IS A COMPREHENSIVE MANUAL FOR MOBILE APP SECURITY TESTING AND REVERSE ENGINEERING FOR IOS AND ANDROID MOBILE SECURITY TESTERS
- TEACHING ENVIRONMENTS: JUICE SHOP, A DELIBERATELY INSECURE SITE FOR DEVELOPERS AND SECURITY TEAMS TO LEARN FROM; INCLUDES TRAINING
- GUIDELINES: CURRENTLY OVER 200 TOTAL PROJECTS

API SECURITY

- APIS EXPOSE APPLICATION LOGIC AND SENSITIVE DATA
- API BREACHES ARE BECOMING MORE PREVALENT
- USE TOKENS FOR AUTHORIZATION AND AUTHENTICATION TO HELP SECURE API CONNECTIONS
- USE AN API GATEWAY WHICH EXPOSES DIFFERENT APIS FOR DIFFERENT CLIENTS AND VERIFIES REQUESTS FROM CLIENTS

WORK WITH THE PROJECT MANAGEMENT OFFICE

- ALL PROJECT PROPOSALS MUST BE REVIEWED BY INFOSEC AT PHASE 0
- WORK WITH THE PMO TO HAVE INFORMATION SECURITY QUESTIONS AS A PART OF THE PROJECT CONCEPT PROPOSAL FORM
- HAVE INFOSEC QUESTIONS AS A PART OF ALL FOLLOW-UP QUESTIONNAIRES

WORK WITH THE SYSTEMS OPERATION TEAM

- ENSURE A GOOD WORKING RELATIONSHIP BETWEEN INFOSEC AND OPERATIONS
- ENSURE THAT THERE ARE SEPARATE SECURE ENVIRONMENTS SET UP FOR DEVELOPMENT, TESTING, QA, AND PRODUCTION
- ENSURE ALL ENVIRONMENTS AND SERVERS ARE BUILT FROM AN UPDATED STANDARD IMAGE
- ENSURE THERE ARE SECURITY GATES FOR EACH ENVIRONMENT

DEVSECOPS

- ALL OF THE ABOVE WILL HELP POISE YOU TO BE QUICK AND INTEGRATED INTO THE DEVELOPMENT PIPELINE
- MUCH IS A CULTURE SHIFT
- AUTOMATE AS MANY SECURITY TESTS AS POSSIBLE
- KEEP CONTAINERS THAT RUN MICROSERVICES ISOLATED FROM ONE OTHER AS WELL AS THE NETWORK

ENFORCE ACCESS MANAGEMENT STANDARDS

- WORK WITH HR TO ESTABLISH PROVISIONING/ DEPROVISIONING PROCEDURES
- ENFORCE CENTRALIZED PROCESS TO APPROVE AND GRANT ACCESS TO SYSTEMS
- ENFORCE DEPROVISIONING PROCEDURES
- PERIODICALLY AUDIT SYSTEMS ACCESS
- REQUIRE TWO FACTORS FOR ALL ADMIN ACCESS, AND ALL USER ACCESS TO MISSION CRITICAL SYSTEMS. CONSIDER MFA FOR EVERYTHING
- NO ONE SHOULD BE REGULARLY LOGGED IN WITH ADMIN PRIVILEGES

EFFECTIVE SECURITY PATCH MANAGEMENT

- HAVE PROCESSES IN PLACE TO ENSURE REGULAR, TIMELY, AND ENTERPRISE-WIDE PATCHING
- TEST PATCHES ON PILOT GROUP
- INCLUDE THIRD-PARTY APPS
- MINIMIZE EXCLUDING ANY SYSTEMS
- MINIMIZE EFFECT ON USERS

ENCRYPT

- EVERYTHING
- EVERYWHERE
  - At rest
  - In transit
- DO NOT MAKE YOUR OWN ENCRYPTION ALGORITHM
- AES IS THE TRUSTED US GOVERNMENT ENCRYPTION STANDARD
- HAVE A WELL THOUGHT OUT AND TESTED KEY MANAGEMENT PROCESS
- DO NOT ALLOW INSECURE PROTOCOLS SUCH AS TELNET OR SSL (USE TLS 1.2)

DIVERSITY IN THE WORKFORCE

- THERE ARE NOT ENOUGH QUALITY DEVELOPERS AND INFOSEC PROFESSIONALS TO ADDRESS THE INCREASING NEEDS OF COMPANIES
- SUPPORT AND ENCOURAGE WOMEN AND MINORITIES
- ENSURE A ZERO TOLERANCE WORK ENVIRONMENT
- LOOK CAREFULLY AT THE LANGUAGE USED IN JOB POSTINGS
- REACH OUT TO AND SUPPORT ORGANIZATIONS SUCH AS THE OWASP WOMEN IN APPSEC, THE INTERNATIONAL CONSORTIUM OF MINORITY CYBERSECURITY PROFESSIONALS, WOMEN'S SOCIETY OF CYBERJUTSU, AND WICYS - WOMEN IN CYBERSECURITY

NETWORK AND COLLABORATE

- ATTEND NETWORKING EVENTS
  - Make New Contacts
  - Share War Stories and Solutions
- ESTABLISH RELATIONSHIPS: FBI CYBER WATCH, NATIONAL CYBER SECURITY CENTRE (NCSC), CSIRT, ETC.
- JOIN ISSA, OWASP, CSA, ETC.
- FORM NEW GROUPS
- LOOK FOR MEETUPS AND SLACK CHANNELS: OWASP, HACKERSHUB, ETC.

KEEP LEARNING

- SUBSCRIBE TO US-CERT, MS-ISAC, AND VENDOR ALERTS
- WEBCASTS
- BLOGS
- PODCASTS
- CLASSES
- BOOKS
- LINKEDIN AND TWITTER LINKS

HELP PREPARE THE NEXT GENERATION OF SECURITY LEADERS

- HIRE STUDENTS
- TRAIN AND MENTOR YOUR STAFF
- SPEAK AT SCHOOLS
- SUPPORT CYBER COMPETITIONS
- HELP SCHOOLS WITH THEIR CURRICULUM
- TEACH SECURITY AT SCHOOLS

THANK YOU

Richard Greenberg, CISSP

Influencer | Advisor | CISO | CEO | Speaker | ISSA Hall of Fame, Di...

RG.NYLA@GMAIL.COM