ADVENTURES IN DRUPAL SECURITY

JUNIOR TIDAL
WEB SERVICES & MULTIMEDIA LIBRARIAN
NEW YORK CITY COLLEGE OF TECHNOLOGY
@JUNIORTIDAL
ORGANIZATIONAL INFORMATICS
HUMANS ARE FLAWED
HUMANS CREATE SYSTEMS
SYSTEMS ARE INHERENTLY FLAWED
EVENTUALLY SYSTEMS FAIL
THERE IS NO PERFECT SYSTEM
THERE IS NO PERFECT SYSTEM

...SO DON’T TRY TO CREATE ONE.
SYSTEMS FAIL FROM INTERNAL AND EXTERNAL FACTORS
INSTEAD OF BUILDING A PERFECT SYSTEM
EMPHASIZE PREVENTIVE MAINTENANCE
CREATE RECOVERY STRATEGIES
WHAT ARE WE TALKING ABOUT TODAY?

BACKGROUND
SECURITY COMPROMISED!
RECOVERY
LEARNING
SECURING YOUR SITE
BACKGROUND
URSULA C. SCHWERIN LIBRARY SUPPORTS OVER 17,000 STUDENTS OF THE NEW YORK CITY COLLEGE OF TECHNOLOGY (CITY TECH)
ONE OF THE 23 CAMPUSES OF THE CITY UNIVERSITY OF NEW YORK (CUNY)
CONSIDERED A "COMMUTER" SCHOOL
SERVES A DIVERSE POPULATION IN DOWNTOWN BROOKLYN
THE WEB SERVER
MIGRATED FROM A MULTI-DEPARTMENTAL WINDOWS IIS SERVER TO A DEDICATED LAMP SERVER IN 2008.
AD HOC SUPPORTED BY COLLEGE IT DEPARTMENT.
THE WEB SERVICES LIBRARIAN AND IT ASSOCIATE ARE ADMINS FOR THIS SERVER
DRUPAL IS THE CMS USED TO MANAGE SEPARATE DESKTOP AND MOBILE SITES.
DRUPAL 6 WAS USED FOR THE DESKTOP SITE.
USING ANALYTICS INFORMATION, THERE WAS A NEED TO SUPPORT MOBILE USERS.
DRUPAL 7 WAS USED TO CREATE A SEPARATE MOBILE SITE.
CONVERSION FROM D6 TO D7 WASN’T POSSIBLE DUE TO LACK OF SUPPORT OF KEY MODULES
MOBILE SITE
THE MOBILE SITE HAD A WIDGET TO SEARCH THE CATALOG
LINKS TO MOBILE FRIENDLY ELECTRONIC RESOURCES
LIBRARY INFORMATION SUCH AS HOURS AND CONTACT WAS ALSO PROVIDED
SECURITY COMPROMISED!
THE MOBILE SITE WAS HACKED ON DECEMBER 21ST, 2014.
THE BBC REPORTED A DRUPAL HACK ATTACK ON OCTOBER 31, 2014.
UNIVERSITY IT CONTACTED CAMPUS IT ABOUT THE BREACH
THE SITE WAS DEFACED AND THE HOMEPAGE REPLACED
IT DISCONNECTED THE LIBRARY’S SERVER
ATTACK ANALYSIS
AFTER EXAMINING LOG FILES, THERE WASN’T ANY EVIDENCE OF UNAUTHORIZED USERS OR FILES
SEARCHING MYSQL TABLES
FOUND NO MALICIOUS CODE
THE BREACH WAS EITHER THE OUTDATED D7 CORE OR MODULE(S)
THE MOBILE SITE WAS SHUT DOWN
UNTIL THE BETA SITE WAS READY, TRAFFIC WAS REDIRECTED TO THE DESKTOP SITE
LESSONS LEARNED
DON’T NEGLECT YOUR SITE
USE DRUPAL’S EMAIL NOTIFICATIONS FOR NEW UPDATES
IMPLEMENT DRUPAL SECURITY MODULES
DRUPAL SECURITY MODULES
DRUPAL SECURITY KIT
CAPTCHA
BACK UP AND MIGRATE
AUTO LOGOUT
LOGIN SECURITY
DRUSH
STRATEGIES FOR A SECURITY BREACH
CREATE RECOVERY GUIDELINES
CREATE RECOVERY GUIDELINES
TAKE YOUR SITE OFFLINE
MAKE A BACKUP OF YOUR HACKED SITE
REPLACE A HACKED SITE WITH A BACKUP OR FAILOVER SITE
CHECK LOG FILES
NOTIFY ALL WHO NEED TO KNOW
CHANGE PASSWORDS
DOCUMENT EVERYTHING
PREVENTIVE STRATEGIES AT THE SERVER LEVEL
USE HTTPS (PORT 443)
MANAGE FILE EXTENSIONS
MANAGE PHP EXECUTION WITHIN YOUR UPLOADS FOLDER
ROBOTS.TXT
SECURE FILE PERMISSIONS
MAKE AND AUTOMATE BACKUPS
PREVENTIVE MAINTENANCE
STRONG PASSWORDS
EVALUATE USER ROLES AND PERMISSIONS
EXAMINE SUB DIRECTORIES FOR RANDOM FILES ESPECIALLY /FILES AND /UPLOADS
WRAPPING UP
SYSTEMS FAIL
BACKGROUND OF CITY TECH
SECURITY COMPROMISED!
RECOVERY
LEARNING FROM THE COMPROMISE
SECURING YOUR DRUPAL SITE
RESOURCES

DRUPAL’S SECURITY ADVISORIES

YOUR SITE GOT HACKED. NOW WHAT?

SEC4LIB LISTSERV
THANKS!