Cyber Security for Programmers

Basic Concepts
Story: Executive Protection School

Your Number One Threat
You

Your Number Two Threat
Working for a crappy company.
    Companies that duct tape solutions have a nasty habit of failing

Requirements for an Incident
Vulnerability
Vector
Attack

Documentation and Planning
Document what you've done and why for the next generation.
    Maintain and update documentation

90% of time goes to planning and 10% towards implementation.

Procedures
    What happens when events happen?
    Process for communicating with Vested Interests

Periodically verify documentation and procedures. Did a Point of Contact go out on parental leave, how would you find out?

Make sure your documentation is accessible if you have a "biblical flood"

Resources
What resources have you been provided for security?

Build security around the resources that you have, not what you wish you had.

Build based off of institutional capabilities not on specific employee skills.
    What happens if your expert gets poached and no one else understood what they did?

Build buy in with vested interests.
    Ask how the directors kid did at the lacrosse game, and... then ask if they saw the news about a data center going up in flames...

What is Security?

Zimbabwian Ninja Hackers
Dumb Employees
Pissed Off Employees
Paid Off Employees
Employees...
Natural Disasters
Hardware Failures
Vendor Failures
Over Complicated Security Systems
Government Punishments

... someone yanks the wrong plug... ...

Good security will protect from ninja hackers and floods.

Over Complicated Security

Story: Publishing Company
Story: CEO and ISA Server

Resource Constraints are Real

Story: Find me the utility room...

Stupid Employee Games

Story: the 9 level arrays...

Actual Events

Data Center Burned Up:
https://www.datacenterdynamics.com/en/analysis/ovhcloud-fire-france-data-center/
Before dawn broke, fire had ripped through the building. Its bright cladding was a misshapen, smoldering shell. The 30,000 servers inside were destroyed, and the adjacent SBG1 was terminally damaged. Data was lost, and companies across the Internet were reeling. At the height of the fire, 3.6 million websites corresponding to 464,000 domain names were unavailable.

Twitter Hacked:
https://www.npr.org/2020/07/31/897815039/florida-teen-charged-as-mastermind-of-massive-twitter-hack
Twitter has said the hackers used a phone "spear phishing attack" to trick Twitter employees to turn over information that gave the attackers access to internal systems.

Asheville Fiber Lines:
https://www.asheville.com/news/2024/10/buncombes-blackout-severed-fiber-lines-made-it-impossible-to-call-text-or-use-data-on-phones/
Nearly 70 percent of western North Carolina's cell phone towers and equipment were out of service as of Sept. 30, leaving hundreds of thousands with limited or no cell phone signal, according to federal communications data.
Almost all of the towers withstood the damaging winds from Hurricane Helene, but fiber optic lines severed primarily by fallen trees caused a widespread, catastrophic blackout.

We are at WAR!

GOT COUNTER INTELLIGENCE CAPABILITY???

Story: Spiceworks Interview

Suadi Spy at Twitter:
https://www.nbcnews.com/tech/security/former-twitter-employee-sentenced-three-years-prison-spying-saudi-arab-rcna61384
A former Twitter employee found guilty of spying on users on behalf of the Saudi royal family has been sentenced to three and a half years in prison.
Ahmad Abouammo, a dual U.S.-Lebanese citizen who helped oversee media partnerships for Twitter in the Middle East and North Africa, was part of a scheme to acquire the personal information of users, including phone numbers and birth dates, for a Saudi government agent.

China Installs Viruses on New Hard Drives:
https://www.zdnet.com/article/malware-found-on-new-hard-drives/
Following findings by the Investigation Bureau that portable hard discs produced by US disk-drive manufacturer Seagate Technology that were sold in Taiwan contained Trojan horse viruses, further investigations suggested that "contamination" took place when the products were in the hands of Chinese subcontractors during the manufacturing process.

NSA Compromises Hardware In Route:
https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/
A document included in the trove of National Security Agency files released with Glenn Greenwald's book No Place to Hide details how the agency's Tailored Access Operations (TAO) unit and other NSA employees intercept servers, routers, and other network gear being shipped to organizations targeted for surveillance and install covert implant firmware onto them before they're delivered.

Hactivist Nukes Russian Servers with Python Module:
https://arstechnica.com/information-technology/2022/03/sabotage-code-added-to-popular-npm-package-wiped-files-in-russia-and-belarus/
the node-ipc author pushed a new version of the library that sabotaged computers in Russia and Belarus, the countries invading Ukraine and providing support for the invasion, respectively. The new release added a function that checked the IP address of developers who used the node-ipc in their own projects. When an IP address geolocated to either Russia or Belarus, the new version wiped files from the machine and replaced them with a heart emoji.

"War" Footing

Target Acquisition - Do employees post your information to LinkedIn

Off Site Security - Do you audit security of remote workers environments?

Personnel Investigations - If your junior admin buys a multi million dollar house in the Bahamas would you know?

Vendor Trust - Have you ever visited your vendors facilities for at least a sniff test?

Counter Intelligence - Do you know why or if your organization is considered a valuable target?

Target Hardening - Who can update systems and what is the validation process of updates?

audit... Audit... AUDIT... **AUDIT!!!**
    You can't fix problems you don't bother to find...

Disaster Recovery
SAFE DATA IS NOT THE SAME AS USABLE DATA

How much is your companies time worth?
    Data that is "safe" but unusable for a day might be very expensive

Talk to your executives!

DR vs. Backups
Backups are simply data stored in a transportable, stable format.

Disaster Recovery is the process of making services available after a disaster.

How long does it take 10TB to restore???

Disaster Recovery Systems
Replication
Database or data replication between servers and sites that should allow for compromised systems to be taken offline "seamlessly"

Virtual Server Replication
Veeam - Have your servers backup as usable VM's that can be spun up somewhere else.

Hybrid Architecture
Multi Cloud or Public/ Private Cloud Hybrid - What happens if your vendor burns up? or just drops for a few hours?

Physical / Operational Security and Surveillance
Good security keeps well intentioned employees from doing something stupid...

Physical Security
Physically preventing people from accessing hardware.

Doors
Locks
Fences
Server Racks
Server or Device Boxes

Operational Security
Prevent unauthorized people from understanding how your organization and infrastructure works.

Put a "Restroom Out of Order" sign on the server room door (that's locked)

Security through obscurity is a horrible concept that kinda works.

Story: PBX Cards being stolen

Surveillance
Surveillance is not security. You can watch someone steal your servers...

Deterrence - Hidden cameras suck at deterrence

Actionable Intelligence
- Is anyone watching the cameras
- If the person watching the cameras sees an incident do they know what to do?

API Security
Vendor Trust
Who works for the Vendor?

What Happens to Your Data?
- Is "meta" data important?

Key Security
Key Rotation

Don't Upload Your Keys!
- Environment variables

Cache Responses
Caching API request and response pairs allow you to query your own database in the future for perviously acquired data. This allows for continued operations if vendor goes down, and also reduces requests to API during normal operation.

Vendor Shut Down
What happens if your vendor goes offline
- Preconfigure failover to other API vendors, and test while everything is working.

Architecture for Security
Beware of Shadow IT
An employee can circumvent all of your security for $5 a month...

Get buy in from users so that hey use the proper systems.

Understand user problems and try to make your systems work so they don't want to bypass them.

Layered Security
Security should be created in layers with the eye towards if one layer fails that the systems will still be secure. If someone has the admin username and password, but port 22 is blocked the server remains secure.

No Root for Standard Usage
Malware/ viruses can perform tasks based on the users level of access. If the target of a phishing attack can't add a printer then the attack will probably fail.

Don't login as a Global Admin to check your email

Directory Tree Security
Can an attack get to your database file?

Ransomeware doesn't need MySQL privileges if you can just encrypt the whole file.

Permissions and Security
Almost all services allow for some type of permissions scheme. Make sure to fully utilize it on all layers of your application. The OS user account should be locked down, and the account used to query the database should have the specific privileges required for its task.

Caching
Reduces the number of requests to API vendors.

Provides some redundancy if API is unreachable

Make sure your cache is secure. Don't use SQLite on real systems.

Layered Networks and Firewalls
You can't ping what you can't access.

Services vs Servers
If you run the server whether physical or VPS you are responsible for everything from the service configuration, to the os updates, to the CPU fan.

Services decrease the plane of attack against your systems from your perspective. Depending on the vendor there may be a large plane for attack on their side.

Anything that can ping Google is on the "cloud".

Geo Blocking and Auto Blocking
Is there a reason someone in Zimbabwe should log into your systems?

Fail2Ban (https://github.com/fail2ban/fail2ban)
    Auto configures firewall based on rules

Authentication to Systems
SSH Key instead of passwords

MFA (Multi Factor Authentication)

Firewalls for SSH

Encryption
In rest and in transit

Encrypt communications between your own systems.

Certificate rotation

Auditing
You can't fix problems you don't see.

Old Accounts
Inappropriate Permissions
Patch, Updates and Security Settings
Code Reviews

Employees and Contractors
"We hire to quickly and fire too slowly..."

What are the expectations for new hires?
    What is a win, or a loss?

Do they have enough supervision?

Do you have a trusted party that can verify their work?

What documentation and procedures do they have that they can follow?

Story: $200,000 of code that didn't work and the Technical Cofounder couldn't read

Data Fetish
The data you don't have can't be compromised

Is data really the "new oil"? If so why do my Ads still suck?

Articulate a reason that you are collecting the data that you do.

Do other things correlate to PID (Personal Identifiable Information)

Hashing Data
Allows you to test data without seeing what it actually is.
Used for Passwords, but can also be used for things like IP Addresses

Regulations and Laws
PCI, HIPPA, GDPR

Governments will only get stricter about regulations. Do you understand for your target demographics what the regulatory environment looks like?

Paying for services that are compliant may be cheaper than rolling your own.

Just because you web app can be accessed from anywhere doesn't mean you want it to be.

Buy In

Without buy in from vested interests your work will be brutally difficult.

You need the resources and authority from execs to be able to build, deploy and maintain solutions. They need to trust you even when they can't see why.

Story: If the systems work too well they'll fire me

You need the supervision services of mid level managers to make sure procedures are bing followed by employees.

You need mid level managers to respect you enough that they don't just swipe a credit card and create their own "shadow IT"

You need employees to not actively try to circumvent your systems, and to be able to tell you when they see problems.

Office Politics

Know kids names, and what types of dogs people have.

CEO's sign the checks. Secretaries write them...

Talk about anything in the world other than tech with fellow employees. You're not a geek, you're just a peer in a different department.

Understand what your company does and how
offer to buy execs and warehouse workers a cup of coffee so that you can better understand what they do.

Education and Made Up Positions

Run brown bag security briefings/ classes for employees.

Everyone loves pieces of paper. Create your own "Uber Cyber Security Admin" certificate that employees can "earn"

People love gold stars. Create "Cyber Security Liaison" role for departments, and then do brown bag trainings, or debriefing sessions.

Gamify your employees not destroying your systems...