From Setback to Security

Navigating Data Loss in AWS

Justin Keiser

- Drupal Web Programmer
- Academy of Model Aeronautics
- Muncie, IN
- Keiserjb on the Internets

Agenda

- Background
- The Day Our Photos Disappeared
- Recovery
- Backup Strategies
- Prevention

Background

- Lots of websites
- Lots of images
- Hosting
- S3 File System Module

The Incident

Hello there,

%100 of Your S3 files, databases .... have been exfiltrated to our server. (With proof 274 GB)

In order to prevent their permanent deletion, you will need to make a payment in Bitcoin to our Address.

Note that if you do not make the payment, your files will be deleted and you will not be able to recover them.

Once we receive the payment, we will provide you with the download link for all the files.

To negotiate with us for recovery, contact us here:

s3-files@onionmail.org

	DeleteBucket	August 26, 2023, 11:23:41 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	amafoundation
	PutBucketVersioning	August 26, 2023, 11:23:20 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	library-modelaviation
	DeleteBucket	August 26, 2023, 11:23:12 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	modelaviation
	PutBucketVersioning	August 26, 2023, 11:22:46 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	modelaviation
	DeleteBucket	August 26, 2023, 11:22:43 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	dev-ama
	PutBucketVersioning	August 26, 2023, 11:22:24 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	dev-ama
	DeleteBucket	August 26, 2023, 11:22:15 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	districtvi
	DeleteBucket	August 26, 2023, 11:22:07 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	districtvii
	DeleteBucket	August 26, 2023, 11:22:00 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	districtx
	DeleteBucket	August 26, 2023, 11:21:48 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	efs-backup-devpanel-resource-csf1h4su-fs-af7c9fd4
	DeleteBucket	August 26, 2023, 11:21:44 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	efs-backup-devpanel-resource-hufy27c0-fs-53eb2d28
	DeleteBucket	August 26, 2023, 11:21:37 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	library-modelaviation-backup
	DeleteBucket	August 26, 2023, 11:21:24 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	efs-backup-devpanelresource-hbcs13sa-fs-5c39d927
	DeleteBucket	August 26, 2023, 11:20:22 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	efs-backup-devpanel-resource-suhss12s-fs-4743a03c
	DeleteBucket	August 26, 2023, 11:17:57 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	nats.modelaircraft
	DeleteBucket	August 26, 2023, 11:17:49 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	parkpilot
	PutBucketVersioning	August 26, 2023, 11:17:45 (UTC...	drupal-s3	s3.amazonaws.com	AWS::S3::Bucket	parkpilot
	DeleteTags	August 26, 2023, 09:55:45 (UTC...	16920722952894...	ec2.amazonaws.com	-	-
	DeregisterTargets	August 26, 2023, 09:55:10 (UTC...	16920498012858...	elasticloadbalancing.amazonaws.com	AWS::EC2::Instance, A...	i-0422c3d8759bda9fe, arn:aws:elasticloadbalancing:us-east-2:84396...

Impact

- Images gone
- Websites still worked
- Backups?

Initial Recovery

- Plug the hole
- Rebuild buckets
- Upload
- Ransom?

Lessons Learned

- Current Backups
- Public repos
- What is in config?
- Secure the keys

Securing Api Keys

- Key module
- Private repos
- Config ignore
- Keeping secrets out of public repositories

Securing API Keys

- GitHub Actions

  https://docs.github.com/en/actions/security-guides/using-secrets-in-github-actions

- Secret Scanning

  https://docs.github.com/en/code-security/secret-scanning/configuring-secret-scanning-for-your-repositories

- GitLab

  https://docs.gitlab.com/ee/user/application_security/secret_detection/

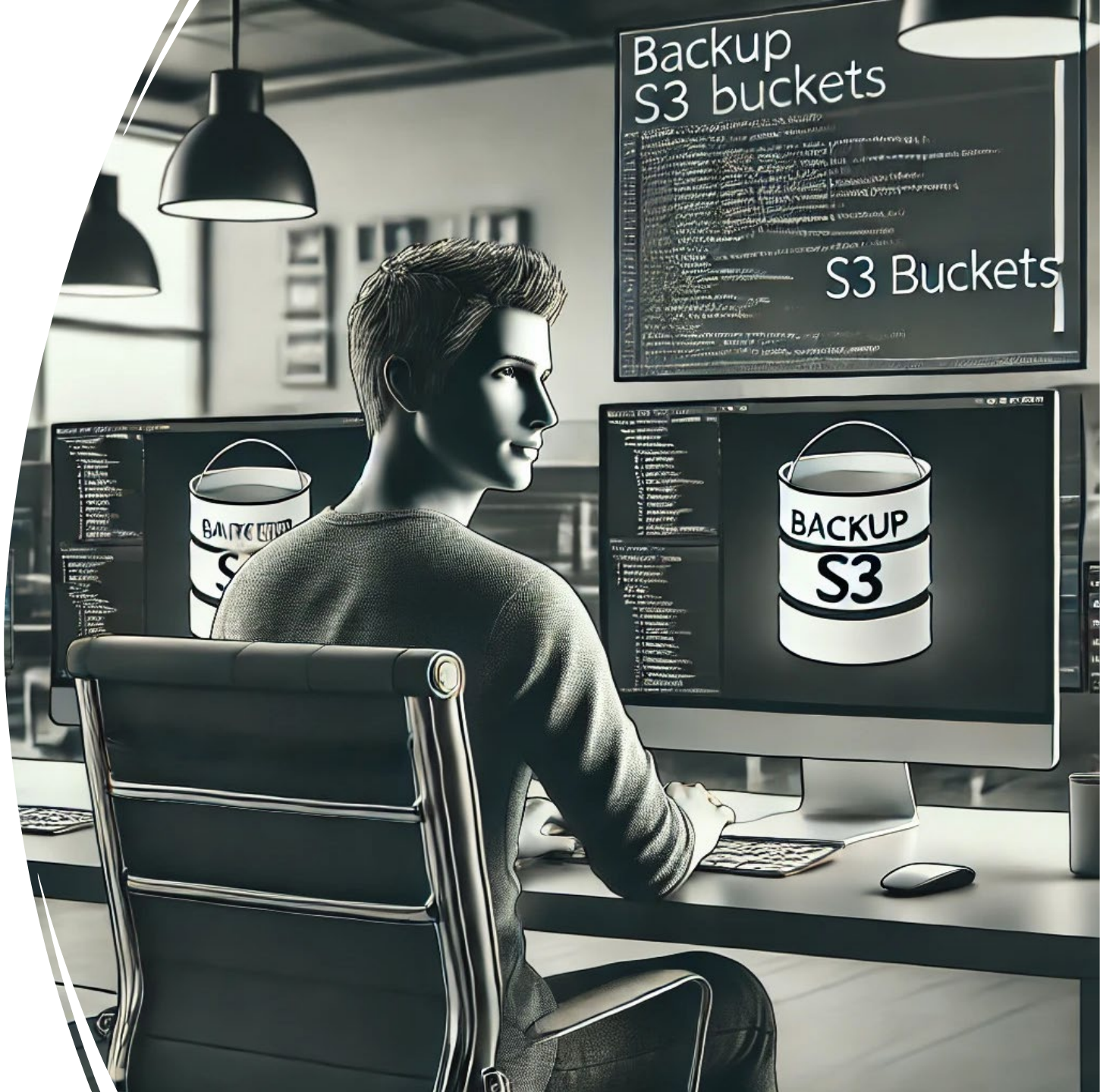
- GitGuardian

- Snyk

Key Module Setup

Automated Backups

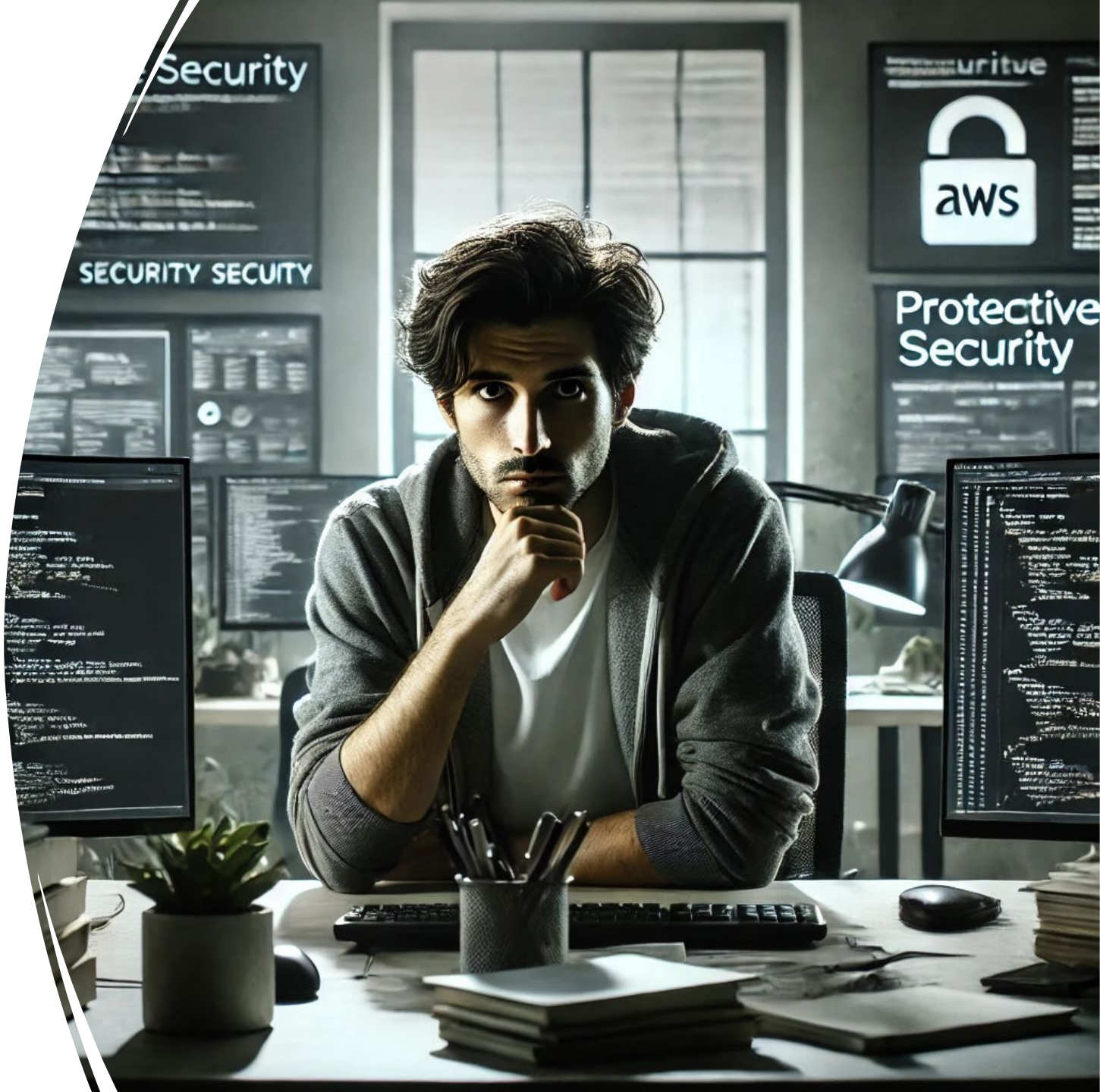
- AWS Backup
- Backup and Migrate
- Backup and Migrate: AWS S3



AWS Backup Setup

AWS and S3 Security

- Create IAM roles for specific tasks
- Look for unauthorized access
- AWS CLI



General Security

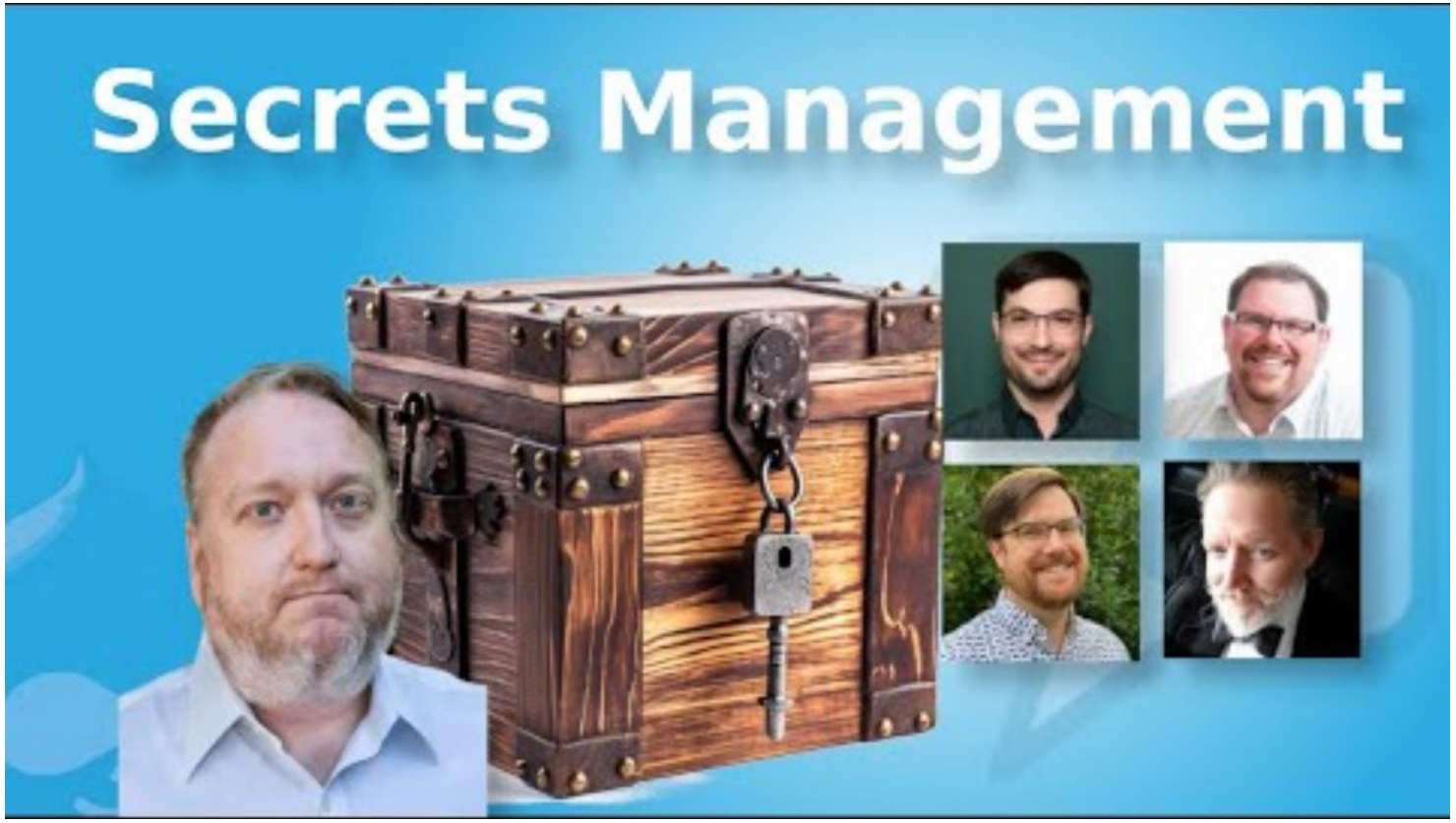
- Security Review
- Security Review B
- WAF
- Malware

Recovery Plan

- What could happen?
- How would I respond?

Talking Drupal #405 - Secrets Management

- https://talkingdrupal.com/405



Questions and Discussion

Key Takeaway

- Don't make the repo public unless you're absolutely sure it's safe.

- Proactively plan for disaster.