#digitalsicher

AKTIONSTAG: DIGITALE SICHERHEIT IM BETRIEB

SESSION:
IHRE WEBSEITE UND IHR ONLINESHOP – ABER SICHER

– WIR ZEIGEN, WIE SIE WEBSEITEN SICHER BETREIBEN UND PRÜFEN GEMEINSAM, WIE SICHER IHR SYSTEM AKTUELL IST.

NRW, 11. MAI 2022, 11:20 – 12:00 Uhr

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

BETRIEB DER WEBSITE

ROOT SERVER

- Volle Kontrolle
- Volle Flexibilität & Verantwortung
- Eigenes geschultes IT Team in-House nötig

MANAGED SERVICE

- Volle Flexibilität
- Daten liegen bei einem Dienstleister
- Verantwortung über Webseite

SaaS

- geringste Verantwortung bzgl. IT-Sicherheit
- geringste Flexibilität
- In-House IT Team meist nicht notwendig

BETRIEB DER WEBSITE

ROOT SERVER

- Volle Kontrolle
- Volle Flexibilität & Verantwortung
- Eigenes geschultes IT Team in-House nötig

MANAGED SERVICE

- Volle Flexibilität
- Daten liegen bei einem Dienstleister
- Verantwortung über Webseite

SaaS

- geringste Verantwortung bzgl. IT-Sicherheit
- geringste Flexibilität
- In-House IT Team meist nicht notwendig

WELCHE SCHÜTZENSWERTE KOMPONENTEN GIBT ES?

NUTZER
- Browser
- Betriebssystem
- Passwörter

SERVER
- Webserver
- Ports
- Betriebssystem

WEBSEITE
- Programmierung
- externe Abhängigkeiten

KOMPONENTE: SERVER

KOMPONENTE: SERVER

KOMPONENTE: SERVER

TLS absichern

- Nur neuste TLS Versionen nutzen
- Alte Ciphern deaktiveren
- Konfigurationsbeispiele unter:

  https://ssl-config.mozilla.org/
- Testen unter:

  https://www.ssllabs.com/ssltest/

KOMPONENTE: SERVER

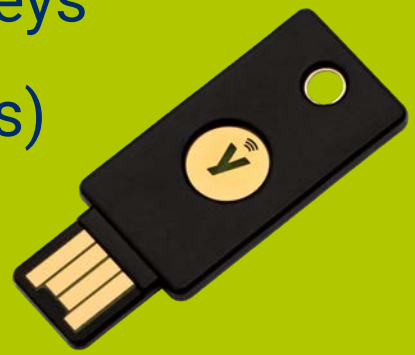
Auswahl des Hosters

- Standort
  - Wo und warum ist das Rechenzentrum da?
- Ausfallsicherheit
  - Sagt der Hoster irgendwas über Ausfallsicherheit?
- Integrität
  - Sind Daten gekapselt von anderen Kunden oder ist es ein „shared“ Hosting?
- Referenzen
  - Gibt es vergleichbare Referenzen?

KOMPONENTE: SERVER

Low Hanging Fruits

- Alle Betriebssystem Updates einspielen
- Firewall (Software oder Hardware) aktivieren und nur benötigte Ports erlauben
- So gut es geht, nah an der Standardkonfiguration von Diensten bleiben
- SSH-Authentifizierung ausschließlich über Pubkeys
  - Noch besser Hardware Tokens (z.B. Yubikeys)



KOMPONENTE: SERVER

Web Application Firewall integrieren

- OWASP Projekt hat vorgefertigte Regeln die mit Nginx und Apache (mod_security) verwendet werden können

Wenn für alles keine Zeit/Budget -> Plesk oder Managed Services nutzen

KOMPONENTE: WEBSITE

SQL Injections vermeiden

- Framework Funktionen für Datenbankabfragen nutzen
- „Never trust user input“
- Dienstleister einfach mal fragen ob danach getestet wird

Trennung zwischen persistenten Daten und Code

- In wp-uploads/ (Wordpress) oder fileadmin/ (TYPO3) gehört kein Code
- PHP Execution für diese Ordner deaktivieren

KOMPONENTE: WEBSITE

Versionsverwaltungs-Dateien nicht öffentlich erreichbar

- Test: https://<domain>/.git/config

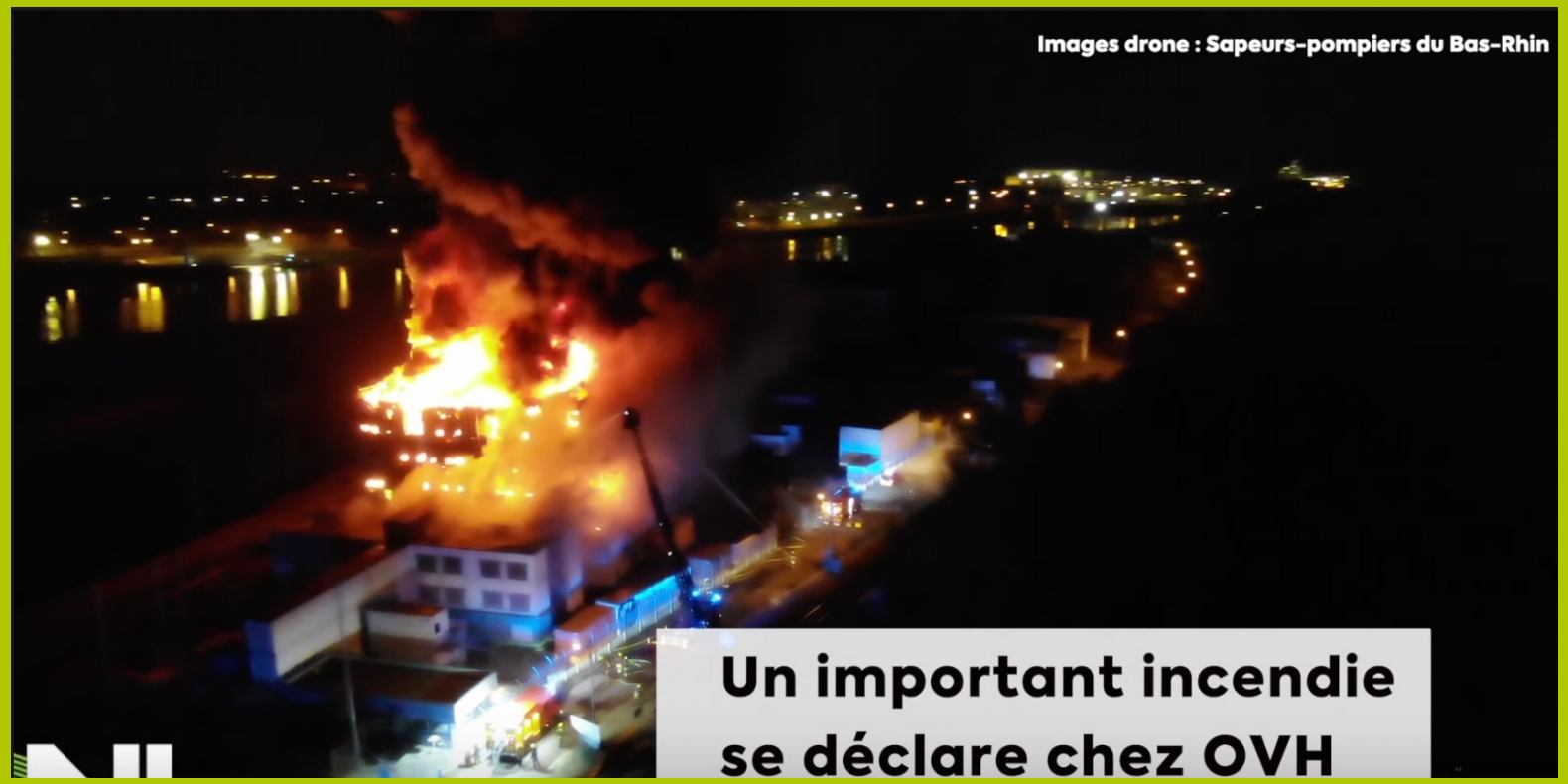
Für Wordpress:

- Einfaches Testing auf Sicherheitslücken mit wpscan

BACKUPS

Nicht nur auf Backups beim Hoster vertrauen

(Snapshots, Automatic Backups, etc)



BACKUPS

Backup selbst erstellen

- Bacula (https://www.bacula.org/)
- Borg (https://www.borgbackup.org/)
- Rsnapshot (https://rsnapshot.org/)

Backups nur verschlüsselt in anderes Rechenzentrum (o.ä.) übertragen

Tipp: Backups nicht vom Webserver aus erreichbar

Mehr Informationen: Session von Niklas Zistler

MONITORING

Modernes Monitoring einsetzen

- Prometheus + Grafana

  (https://prometheus.io/ + https://grafana.com/)
- Icinga (https://icinga.com/)
- Zabbix (https://www.zabbix.com/)

MONITORING

Alerts nicht nur auf Standardwerte wie Speicher, CPU, RAM

- Sondern auch auf Netzwerk Last, User angemeldet, Anwendungsmetriken

Stelle einrichten für das Melden von Sicherheitsproblemen