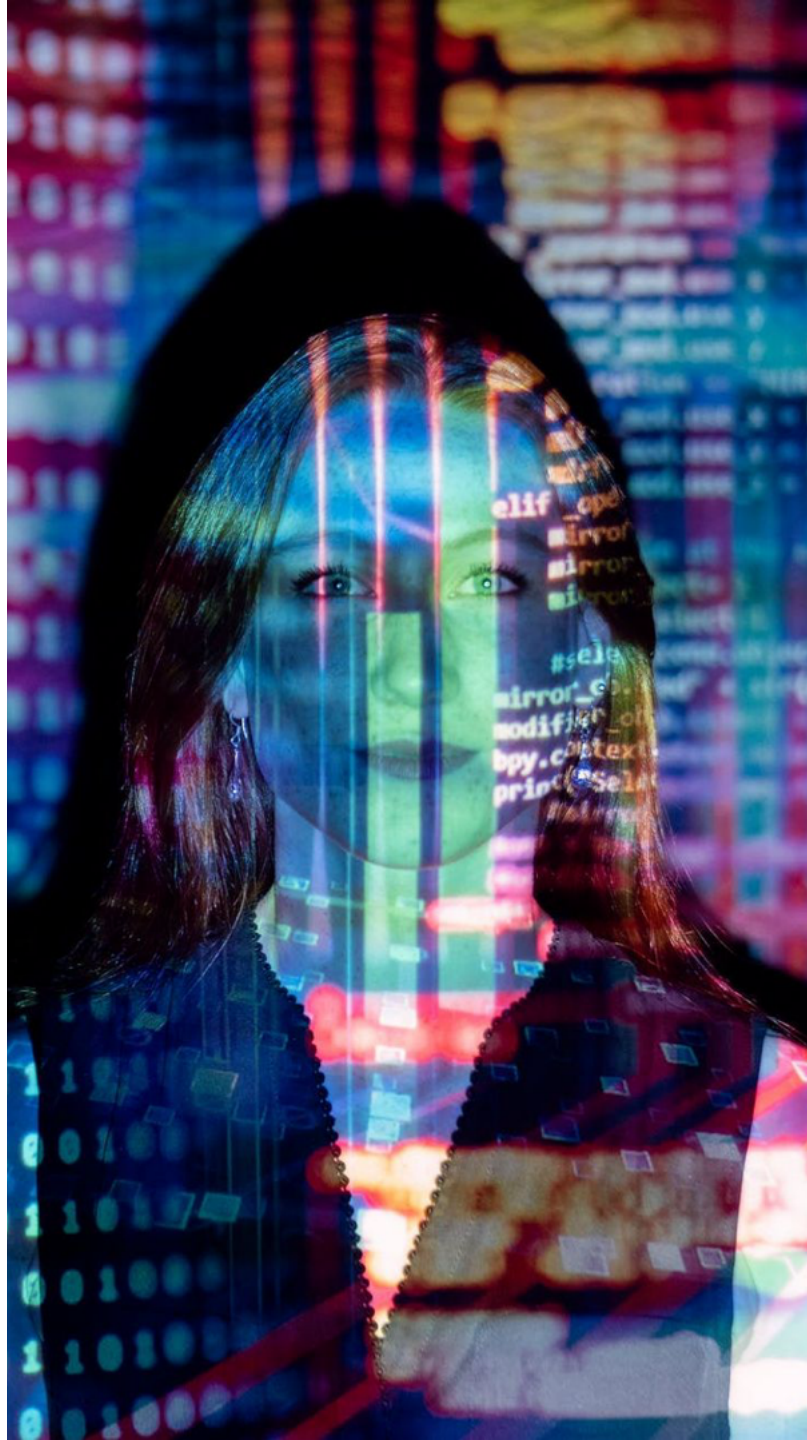
AKTION DEUTSCHLAND HILFT & FUNDRAISINGBOX

Gemeinsam sicher: Cybersicherheit & Online-Fundraising in der Praxis

Andrea Heckmann & Peter Kral

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

FUNDRAISINGBOX



Agenda

1. Begrüßung und Vorstellung
2. A: Cybersicherheit bei ADH
3. Spotlight: Unsere Partnerreise
4. B: Online-Fundraisiung und IT-Sicherheit
5. Austausch und Fragen

Kurze Vorstellung

Andrea

Referentin Online-Marketing | Aktion Deutschland Hilft e.V.

Peter

Gründer & CEO Wikando

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Teil A

Cybersicherheit bei ADH

Bedeutung und Ziele der IT-Sicherheitsmaßnahmen

Keine Chance für Cyberangriffe

Minimierung von Sicherheitsrisiken und Vermeidung von IT Sicherheitsvorfällen.

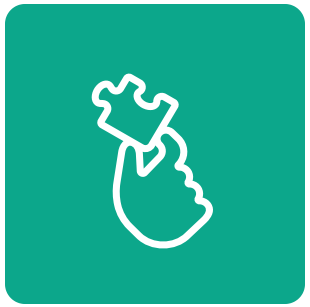
Falls es dennoch passiert?

Wissen was zu tun ist, damit Zugriff auf die eigenen Systeme und Daten schnell wiedererlangt wird.

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Ausgangssituation 2023

Die Puzzle-Teile sind nicht verbunden



Einzelne Silos

Diverse Arbeitsanweisungen zum Thema IT Sicherheit vorhanden

Schulung der Mitarbeiter im Datenschutz, aber nicht explizit im Hinblick auf IT Sicherheit

Wartung und regelmäßige Sicherheits-Updates durch Dienstleister

Fazit

Mangelnder Überblick über Sicherheitszustand der IT Systeme (Status Quo)

Fehlender „Blick von außen“

Eigenes Sicherheitskonzept mit den Komponenten Vorbeugung, Erkennung und Wiederherstellung nicht vorhanden

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Auswahlprozess zur Anbieterfindung

Herausforderung

1. Welche Maßnahmen möchten wir konkret durchführen?
2. Welcher Anbieter bietet das für uns passende Angebot (Leistungsumfang)?
3. Wann können die einzelnen Maßnahme von Seiten des Anbieters durchgeführt werden?
4. Wie hoch sind die Kosten?

Vorgehen

1. Anfrage an insgesamt 11 Anbieter
2. Gespräche in Form von Telefonaten und / oder Web-Meetings mit einzelnen Anbietern, zur Konkretisierung der Inhalte
3. Vergleich der einzelnen Angebote und Auswahl des Anbieters
4. Vertrag- und Terminfindung zur Durchführung der festgelegten Maßnahmen mit dem Anbieter
5. Durchführung der einzelnen Maßnahmen und Auswertung der Berichte

Auswahlprozess zur Anbieterfindung

April Mai 2023

Anfrage und Gespräche mit Anbietern

Juni

Auswertung und Auswahl Anbieter

Sep. - Jan.

Planung und Durch-führung Audit, PEN-Tests, Social Engeneering Angriff

Jan 2024

Schulung der Mitarbeiter:innen

Feb. - Juni

Auswertung PEN-Tests, Behebung Mängel / Sicherheitslücken, Erstellung Leitfaden für Mitarbeiter, etc.

Juli

weitere Maßnahmen folgen

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Durchgeführte IT-Sicherheitsmaßnahmen

1. **IT-Sicherheits-Audit**
   Überprüfung der vorhandenen Netzwerk-Systeme im Aktionsbüro

2. **Infrastruktur-Pentest**
   Überprüfung der IT-Systeme und einzelner Systembestandteile, die öffentlich über das Internet erreichbar sind, also von Dritten angegriffen werden können.

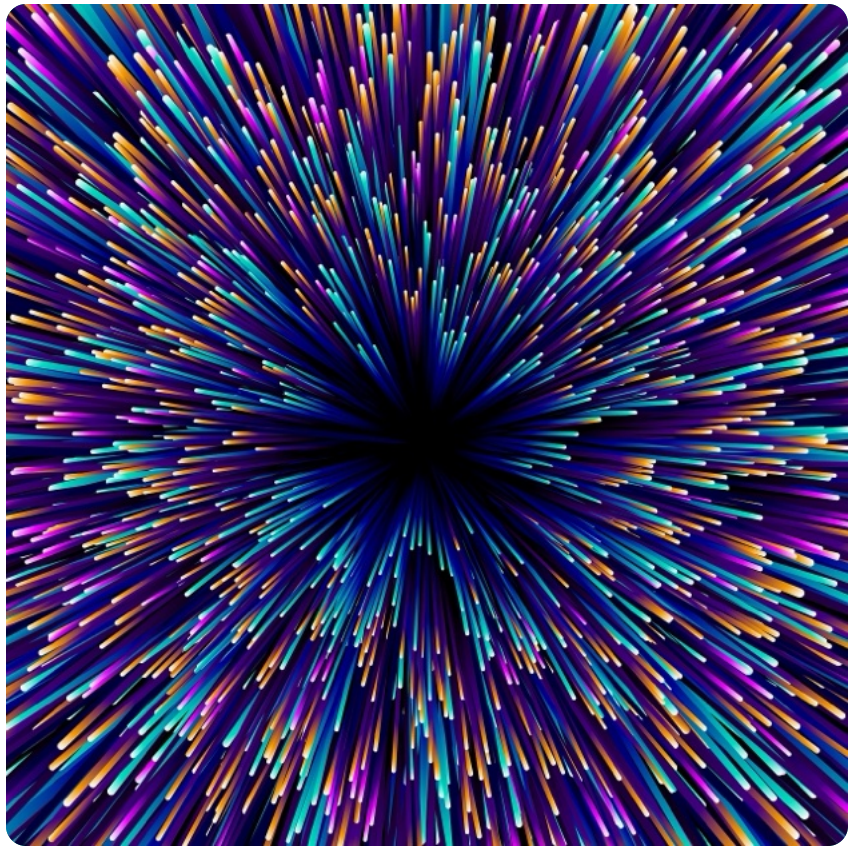
3. **Website-Pentest**
   Überprüfung der Sicherheit der Website durch Simulierung eines Angriffs

4. **Simulierter "Social Engineering Angriff"**
   über Phishing Mail (Social Awareness Kampagne)

5. **IT-Sicherheitsschulung für alle Mitarbeiter*innen**
   Security Awareness - Gemeinsam für Informationssicherheit: Wie verhalte ich mich richtig?

Social Awareness Kampagne

Simulierter "Social Engineering Angriff"



- **Versand einer E-Mail über einen vorgetäuschten Admin-Account** an alle Mitarbeiter:innen mit Handlungsaufforderung, dem Link „Download Passwortrichtlinie“ zu folgen und auf der nachgelagerten Website Benutzernamen und Passwort einzugeben
- Nachgelagerte **Website war eine Dummy-Website**, die vom Layout und Aufbau identisch war mit Webseiten von Aktion Deutschland Hilft
- Die **Erfassung der Kennzahlen** (Klick auf Download-Link, Eingabe von Daten auf Website, Start des Downloads) erfolgte **anonym**. Ein Rückschluss auf einzelne Personen war nicht möglich!

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Ergebnis und Ausblick

Berichtswesen

- zum aktuellen Zustand der Infrastruktur (intern und extern) sowie der Website
- Status Quo der Systemlandschaft, auf dem weiter aufgebaut wird

Training

- Durchführung der IT Sicherheitsschulung

Personal

- Schaffung einer neuen Stelle zur Betreuung des Themas IT-Sicherheit und Datenschutz

IT Sicherheitskonzept

- Erstellung eines IT Sicherheitskonzepts mit den Komponenten
- Vorbeugung,
- Erkennung und
- Widerherstellung

FundraisingBox-Tools

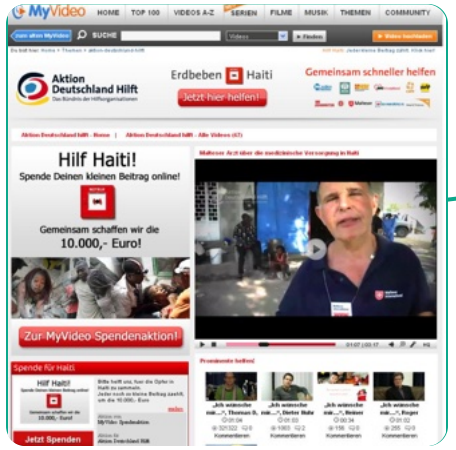
- Weiterer Ausbau und Nutzung von Funktionen und Workflows der Fundraising Box

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Spotlight

Unsere Partner-Reise

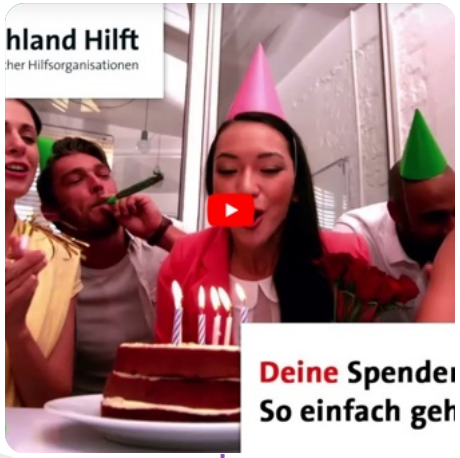
Die Partnerschaft



Die gemeinsame Reise beginnt

2008 Helpedia

Aktion Deutschland Hilft ist auf der ersten deutschen Spenden-Plattform Helpedia



2010 Spendenaktionen

Spender*innen werden zu Fundraiser*innen: Spendenaktionen sind auf der ADH-Website integriert

2021 Form-API Formular

Formulare werden individuell gestaltet: das perfekte Spendenerlebnis

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Seite an Seite...

... bei großen Katastrophen

und bei innovativen Ideen!

2021 Ahrtal Flutkatastrophe

- Bis zu **40** Transaktionen pro Sekunde
- Notfallteam wird geboren
- Backup Systeme werden eingerichtet

2022 Ukraine Krieg

- 100% Erreichbarkeit
- Starke Solidarität & Unterstützung

2022 WDR Charity Aktion

- Spenden mit Wunschsong verbinden, solche Formulare gab es noch nie!

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Eine starke Partnerschaft

Dreistellige Millionensumme

Mit frischen Ideen hat ADH über die Spendenaktionen & Formulare hohe Summen gesammelt.

Gemeinsam Wachstum stärken

Mit 75 Expert*innen bei der FundraisingBox wollen wir weitere Höhepunkte erreichen.

Vertrauen und Sicherheit bewahren

Mit bewährte Notfall- und Peak-Mechanismen können wir neue Herausforderungen meistern.

Teil B

Online-Fundraising und IT-Sicherheit

FundraisingBox

"Vertrauen durch Sicherheit, unterstützt von Experten." Peter Kral

Seit 14 Jahren unterstützt die FundraisingBox weltweit gemeinnützige Organisationen

Über 4 Mrd. Euro in 25 Mio. Transaktionen und tausende zufriedene Kunden.

Wachstum und Erfolg basieren auf Vertrauen und Sicherheit.

Investitionen in Cyber-Sicherheit sind der Schlüssel zu unserem Erfolg

Unsere Sicherheits-maßnahmen schützen uns und unsere Kunden vor Cyber-Bedrohungen

Unsere Teams arbeiten rund um die Uhr für höchste Sicherheit.

Schutz persönlicher und finanzieller Informationen vor Missbrauch und Bedrohungen

Sensibilität der Daten im Online-Fundraising

Zusammenführung von Daten

- Persönliche Daten: Name, Adresse, E-Mail, Telefonnummer
- Finanzielle Daten: Transaktions-Historie, Kreditkarteninformationen, Bankdaten

Missbrauchspotenzial

- Finanzbetrug durch unautorisierte Transaktionen
- Identitätsdiebstahl (Dokumentenfälschung, Kontoeröffnung, Geldwäsche, Terrorismus und organisierte Kriminalität)
- Social Engineering und Phishing
- Einbruch und Diebstahl

Schutz persönlicher und finanzieller Informationen

Risiken und Bedrohungen für Non-Profits

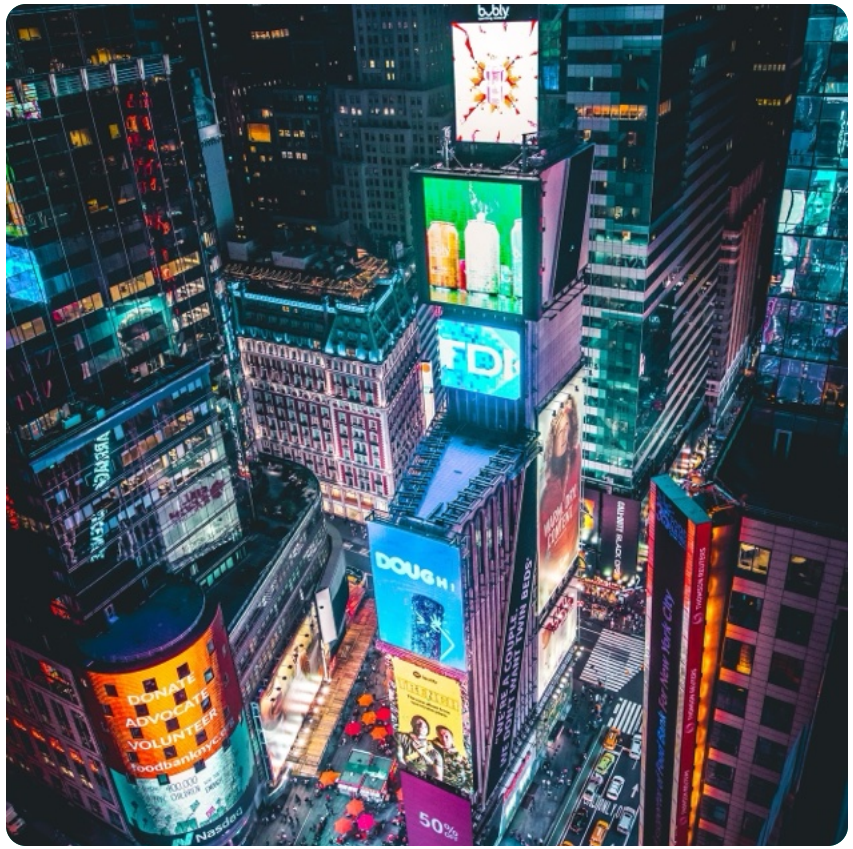


Image-Schaden

Reputationsschaden durch einen öffentlich bekannt gewordener Datendiebstahl kann das Ansehen der Organisation beschädigen.

Vertrauensverlust bei Spender*innen kann zu einem Rückgang der Spenden führen.

Missionserfüllung wird erheblich erschwert.

Schutz persönlicher und finanzieller Informationen

Risiken und Bedrohungen für Non-Profits

Finanz-Schaden

Spendenrückgang: Unterstützende stellen das Spenden ein oder wechseln zu anderen NPOs.

Kosten für Schadensbegrenzung: Untersuchung, rechtliche Beratung, Sicherheitsverbesserungen, Gegenmaßnahmen im Marketing.

Bußgelder und Strafen bei Nichteinhaltung der DSGVO.

Schadensersatz: Klagen und Rechtsstreitigkeiten führen zu zusätzlichen finanziellen Belastungen.

Schutz persönlicher und finanzieller Informationen

Risiken und Bedrohungen für Non-Profits

Störungen im Betrieb

Betriebliche Unterbrechungen: IT-Systeme müssen zur Untersuchung und Behebung des Vorfalls abgeschaltet oder eingeschränkt werden.

Fokusverschiebung: Ressourcen und Aufmerksamkeit müssen auf die Bewältigung des Vorfalls statt auf die Hauptmission gelenkt werden.

Schutz personenbezogener und finanzieller Daten im Online-Fundraising

Best Practices zur Absicherung von Webservern

Die Risiken

Ungepatchte CMS und Plugins sind häufige Angriffsziele, die durch automatische Scans entdeckt werden.

Falsche Konfiguration durch nicht-technische Administratoren

Best Practices

Beschränkter Zugriff: Nur autorisierte ausgebildete Nutzende haben Zugriff.

Geregeltes Update-Management: Zeitnahe Sicherheitspatches, klare Zuständigkeiten, volle Transparenz, Security-Alerts, geschützte Zeitfenster.

Keine einschränkenden Individualisierungen: Gewährleistung der vollen Update-Fähigkeit

FundraisingBox hilft

Abkopplung personenbezogener Daten: Physische Trennung von Website-Datenbank und Spendendaten durch dedizierten Datenbankserver oder spezialisierte Cloud-Dienste (z.B. FundraisingBox).

Sichere Anbindung von Geschäftsprozessen: Entkoppelte Web-Services wie FundraisingBox

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Absicherung des Zugriffs durch Nutzende

Best Practices zur Absicherung der Speicherung persönlicher Daten

- **Least-Privilege Prinzip**: Definierte Rechte-Granularitäten zur Konfiguration und Sichtbarkeit. Zugriffsbeschränkung auf das notwendige Minimum.
- **Audit-Log:** Protokollierung aller kritischen Operationen auf Nutzerebene. Nachvollziehbarkeit und Überwachung von Zugriffen und Änderungen.
- **Restore-Möglichkeit**: Möglichkeit zur Rückgängigmachung kritischer Operationen. Sicherstellung der Datenintegrität und Wiederherstellung.
- **Starke Passwörter und Zwei-Faktor-Authentifizierung**: Durchsetzung von komplexen Passwörtern.Verwendung von FIDO, OTP, Passkeys für zusätzliche Sicherheit.
- **Intrusion-Detection**: Automatische Sperrung von IPs und Accounts bei Brute-Force-Attacken. Schutz vor unautorisierten Zugriffen.

Absicherung der Infrastruktur

Best Practices zur Absicherung des Speicherorts von persönlicher Daten

IAM (Identity and Access Management)

Implementiert Least Privilege

- Strikte Zugriffskontrolle auf AWS-Ressourcen mit IAM-Rollen und -Richtlinie
- Multi-Faktor-Authentifizierung (MFA) für zusätzliche Sicherheit.

Encryption in Transit

Verschlüsselt Datenübertragung mit TLS/SSL

- Schutz vor Abhören und Manipulation durch aktuelle Cipher-Suites und HSTS.

Security by Design und regelmäßige Code Reviews

Sicherheitsaspekte in den Entwicklungsprozess integrieren:

- Nutzung sicherer Programmierstandards
- Regelmäßige / automatische Code-Überprüfungen im CD/CI-Prozess.

VPN, Subnetze, Sicherheitsgruppen und NACLs

Anwendung in sicherer Netzwerkumgebung isolieren:

- Private Netzwerke für interne Daten, öffentliche Netzwerke nur für externe Endpunkte
- Begrenzt Datenverkehr zur Verhinderung unbefugten Zugriffe

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Absicherung der Infrastruktur

Best Practices zur Absicherung des Speicherorts von persönlicher Daten

Encryption at Rest

Verschlüsselt gespeicherte Daten:

- Schutz vor unbefugtem Zugriff und Diebstahl durch Verschlüsselung auf Festplatten und in Datenbanken.

Vulnerability Scanning und Penetration Testing

Automatisierte Tools und simulierte Angriffe:

- Scannen der Web-Applikation und Infrastruktur auf Schwachstellen
- Detaillierte Schwachstellenanalyse durch Experten.

Protokollierung und Überwachung

Erfassung sicherheitsrelevanter Aktivitäten:

- Kontinuierliche Überwachung der Systeme zur Erkennung verdächtigen Verhaltens und frühzeitiger Erkennung potenzieller Angriffe.

Datensicherung und Wiederherstellung

Regelmäßige und sichere Speicherung von Backups in getrennten Umgebungen:

- Plan für schnelle Reaktion auf Sicherheitsvorfälle und Wiederherstellung des Betriebs.

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

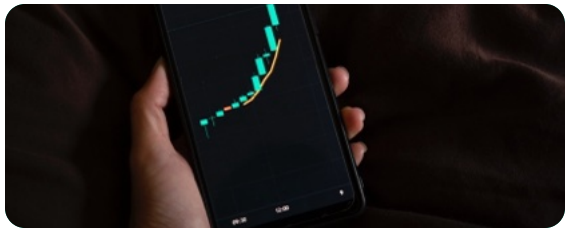
Absicherung der Infrastruktur

Best Practices zur Hochverfügbarkeit

100% Uptime bei bis zu 40 Transaktionen/Sekunde für Aktion Deutschland Hilft e.V.

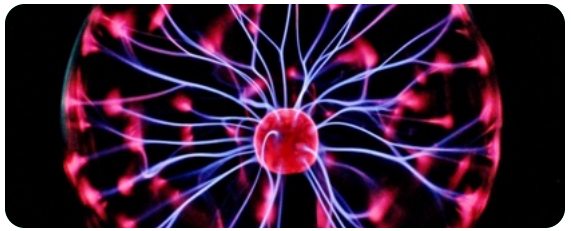
Multi-AZ Deployments

Verteilung der Infrastruktur über mehrere Rechenzentren zur Minimierung von Ausfallzeiten und gleichmäßiger Lastverteilung.



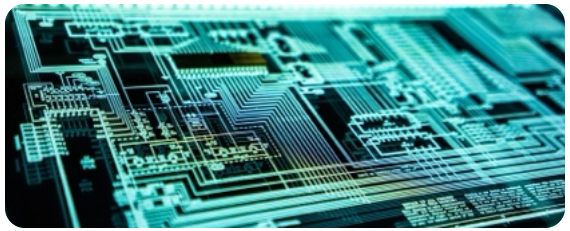
Automatische Skalierung

Anpassung der Server-Instanzen je nach Nachfrage zur Optimierung von Verfügbarkeit und Effizienz durch Auto Scaling.



Alerting und Incident Management

Uptime-Monitoring, automatisierte Alarme für kritische Metriken, und klare Prozesse zur schnellen Reaktion auf Anomalien.



Schutz vor DDoS-Angriffen

Anti-DDoS-Dienste und Web Application Firewall zur Abwehr schädlichen Datenverkehrs.

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Gemeinsam schneller helfen

Suche

2021
Ahrtal

Spenden & helfen

Online-Spenden für die Not- und Katastrophenhilfe

Aktion Deutschland Hilft e.V. und FundraisingBox

Zusammenarbeit in der Krise

Notfallteam

24/7 Bereitschaft, um im akuten Krisenfall auf Naturkatastrophen und andere Ereignisse zu reagieren.

Schnelle Reaktionszeit

Verfügbares Solution-Team, um individuelle, technische Herausforderungen schnellstmöglich lösen zu können.

Direkte Kommunikation

Hochqualifizierte Fachleute der FundraisingBox direkt und in Echtzeit (via Slack) ins Krisenmanagement der Organisation eingebunden.

Partnerschaften nutzen

Nutzung der AWS Ressourcen und dessen Disaster Repsonse Action Team in Krisenfällen

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Amazon Web Services (AWS)

Gemeinsam stark mit AWS und anderen Partnern

- **Skalierbarkeit und Automatisierung**

  Organisationen wie Aktion Deutschland Hilft e.V. oder das Rote Kreuz nutzen Services von AWS.

- **Cloud-Guthaben**

  AWS unterstützt kleine, gemeinnützige Institutionen in Deutschland mit jährlich 1.000 USD. Das Guthaben kann direkt über Stifter-helfen beantragt werden.

- **Andere Programme**

  AWS bietet viele Programme für gemeinnützige Unternehmen an, wie z.B. „Data Lake for Nonprofits“ mit unserem gemeinsamen Partner Salesforce

aws

Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Aktion Deutschland Hilft e.V. und FundraisingBox

Technisches Fallback-System

- **Herausforderungen**

  Im Falle einer längeren Downtime der ADH-Website z.B. durch einen Hacker-Angriff, eines enormen Traffic-Aufkommens oder eines technischen Fehlers, soll es möglich sein, in kurzer Zeit die Verfügbarkeit der Spenden-Seite wieder herzustellen.

- **Lösung**

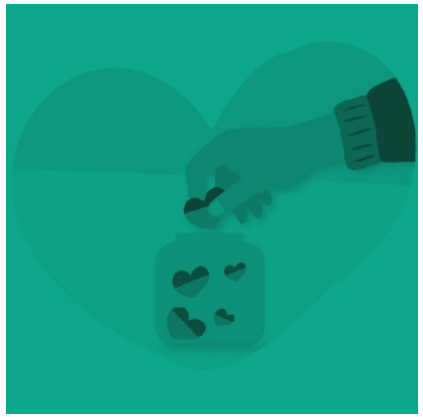
  ADH und wir halten gemeinsam mit Amazon AWS eine vollwertige Fallback-Infrastruktur bereit, die sowohl das Aufrufen der ADH-Webseite, die Zahlungsabwicklung, als auch die Echtzeit-Bedankung bei den Spendenden garantiert.

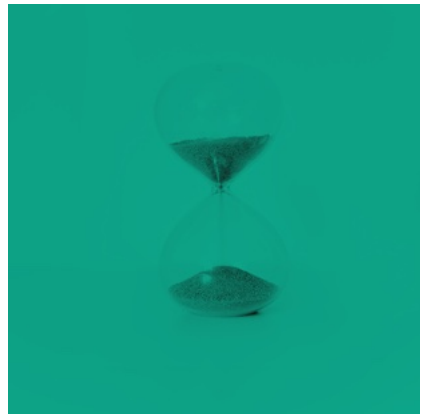
- **Vorteile**

Spendenvolumen absichern

Vertrauen in die Marke stärken

Zeitgewinn für die Wiederherstellung





Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

FundraisingBox unterstützt in Spitzenzeiten

Best Practices zur Peak-Verarbeitung

- **Stabilität am Gipfel:** Wenn unzählige Transaktionen gleichzeitig verarbeitet werden müssen geht es um effiziente Handhabung der Spendenaufkommen.
- **Echtzeit-Kommunikation:** Spendende erhalten sofort eine personalisierte Zahlungsbestätigung per E-Mail; bei Lastschriften umgehend SEPA-Mandat und Pre-Notification.
- **Echtzeit-Zahlungsverarbeitung:** Alle Zahlungen werden in Echtzeit eingezogen, Spenden sind schnellstmöglich verfügbar.
- **Buffering:** Alle eingehenden Daten werden vorverarbeitet und zwischengespeichert. Falls externe Dienstleister nicht erreichbar sind oder dem Peak nicht standhalten können, werden die Daten solange gehalten, bis diese wieder verfügbar sind. Die Verarbeitungs-Geschwindigkeit kann absichtlich reduziert werden, um Partner nicht zu überlasten.

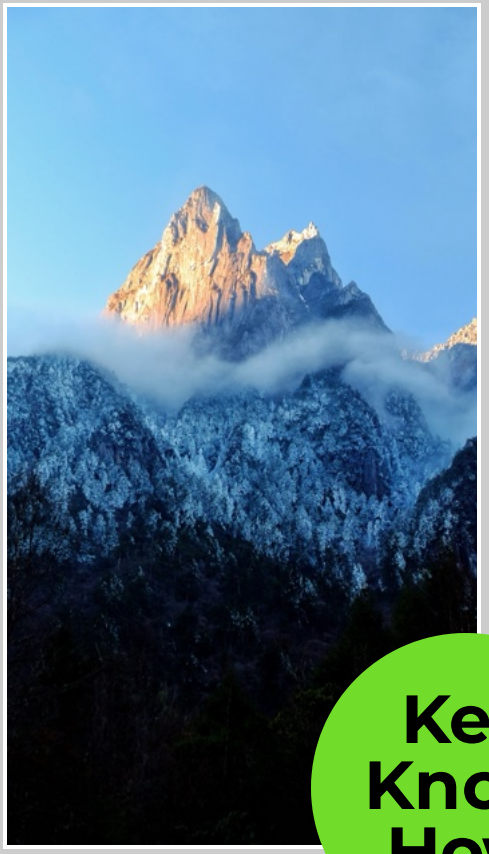
Aktion Deutschland Hilft
Bündnis deutscher Hilfsorganisationen

Abschluss

Austausch und Fragen

Cyber-Security bei FundraisingBox und Aktion Deutschland Hilft e.V.

Aus Sicht des Tech-Entrepreneurs



Key Know How

1 Wachstum basiert auf Vertrauen

Enge Zusammenarbeit zwischen unseren Mitarbeier*innen und Orgas

2 Investitionen in Cyber-Security

Werden immer wichtiger angesichts aktueller Angriffe auf die Zivilgesellschaft

Sind ein Schlüssel zum Erfolg

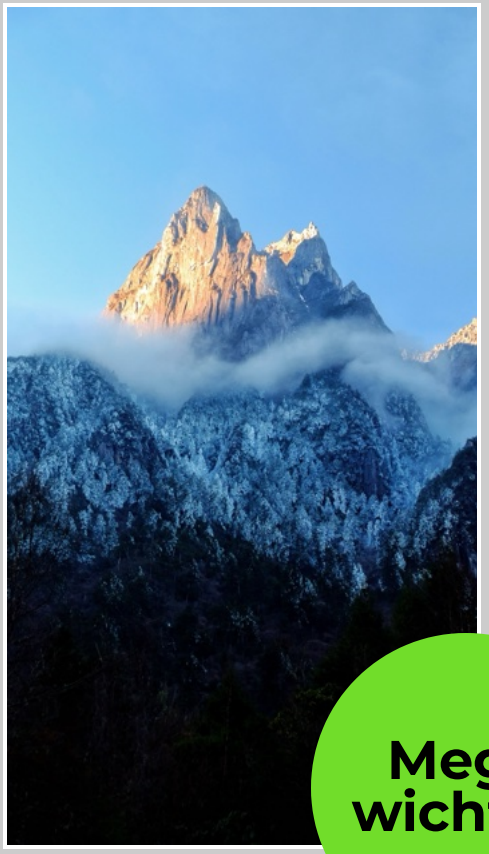
3 Erfahrung ist wichtig

Keine Angst vor hohem Spendenaufkommen

breite Partnerschaften

Cyber-Security bei FundraisingBox und Aktion Deutschland Hilft e.V.

Aus Sicht des Online Marketings



Mega wichtig!

1 Notwendigkeit eines stabilen und sicheren Systems

Verarbeitung eingehender Online-Spenden

Bewältigung von Ausfällen bei der Weiterverarbeitung durch Dienstleister

2 Erhöhte Anforderungen bei Katastrophen

Umgang mit zusätzlichem Traffic durch Online-Werbekanäle

Sicherstellung der Systemverfügbarkeit und -zuverlässigkeit

3 Szenarien, die hohe Systemstabilität erfordern

Versand von Newslettern

Start von Suchmaschinen-Kampagnen

4 Sichere Begleitung der Spender

Von der Dateneingabe im Formular bis zum Versand der Bestätigungs-E-Mail und Spendenquittung

Wir freuen uns, von Dir zu hören.

FundraisingBox

All-in-One-Software für digitales Fundraising

sales@fundraisingbox.com

+49 (0) 821 666 0 9000

fundraisingbox.com