POINTSHARP

Success Story

Schnelle Reaktion auf Phishing-Bedrohungen im Finanzsektor

mit Cryptshare – Secure Information Exchange Automatisierung

www.pointsharp.com



POINTSHARP

Ausgangssituation

Phishing-Angriffe mit finanziellem Schaden nehmen stetig zu. Besonders kritisch: Fälle, in denen Kundinnen und Kunden bereits sensible Daten wie IBANs preisgegeben haben. Für Finanzinstitute entsteht hier ein enormer Zeitdruck — denn je schneller kompromittierte Konten identifiziert und Betroffene informiert werden, desto geringer ist der potenzielle Schaden.

Ziel war es daher, einen automatisierten, sicheren und skalierbaren Prozess zu schaffen, um:

- kompromittierte Daten frühzeitig zu erkennen
- Finanzbetrug zu verhindern
- betroffene Finanzinstitute schnell zu informieren
- und Kunden effizient zu schützen.

Herausforderung

Die größte Herausforderung lag in der Kombination mehrerer Faktoren:

- **Anonyme Quellen** (z. B. eingehende Phishing-Meldungen)
- **Datenvalidierung und Analyse** durch CERT.at
- **Sichere und datenschutzkonforme Weitergabe** an Finanzinstitute
- **Schnelligkeit und Automatisierung**, ohne auf manuelle Prozesse angewiesen zu sein

Gleichzeitig musste berücksichtigt werden, dass CERT.at selbst **nicht direkt für die Kundenkommunikation zuständig ist** — diese Verantwortung liegt bei den Finanzdienstleistern.

> “Mit diesem Projekt haben wir gezeigt, wie schnell und effektiv sich aus Threat Intelligence ein konkreter Schutz für Kunden entwickeln lässt – automatisiert, skalierbar und in enger Zusammenarbeit mit starken Partnern.
>
> Durch die konsequente Automatisierung und die Integration unserer Systeme konnten wir einen durchgängigen Prozess schaffen – von der Erkennung bis zur Handlung, ohne Medienbrüche.”
>
> Wolfgang Menezes,
> Information Technology Security Analyst, CERT.at

POINTSHARP

Die Lösung

Innerhalb von nur **einem Monat** wurde eine leistungsfähige Lösung implementiert — mit **Go-Live**. Die Architektur basiert auf einer intelligenten Kombination mehrerer Systeme:

Zentrale Komponenten

- **IntelMQ (CERT.at Eigenentwicklung)**: Analyse- und Datenbereitstellungstool
- **RT (Ticket-System)**: Steuerung und Nachverfolgung von Fällen
- **Cryptshare Enterprise Edition**: Sichere Übertragung sensibler Informationen mit Automatisierung
- **API-basierte Integration**: Automatisierte Kommunikation zwischen allen Systemen

Prozessablauf

1. Ein anonymer Hinweis auf Phishing oder Finanzbetrug geht ein
2. CERT.at prüft und validiert die Daten
3. Relevante Informationen (z. B. kompromittierte IBANs) werden analysiert und angereichert
4. Über **IntelMQ** erfolgt die strukturierte Aufbereitung und ggf. Bündelung nach Finanzinstituten
5. **Cryptshare** überträgt die Informationen sicher via API an die jeweiligen Finanzinstitute
6. Die Finanzinstitute informieren ihre betroffenen Kunden

Wichtig:
Dabei werden **keine unnötigen Detail-daten offengelegt**, sondern lediglich die relevanten Zuordnungen, um schnell han-deln zu können.



POINTSHARP

Besonderer Mehrwert

Hoher Automatisierungsgrad
Manuelle Zwischenschritte werden minimiert — Daten werden automatisiert geprüft, aufbereitet und übermittelt.

Schnelligkeit & Effizienz
Die Zeit zwischen Erkennung und Benachrichtigung wird drastisch reduziert.

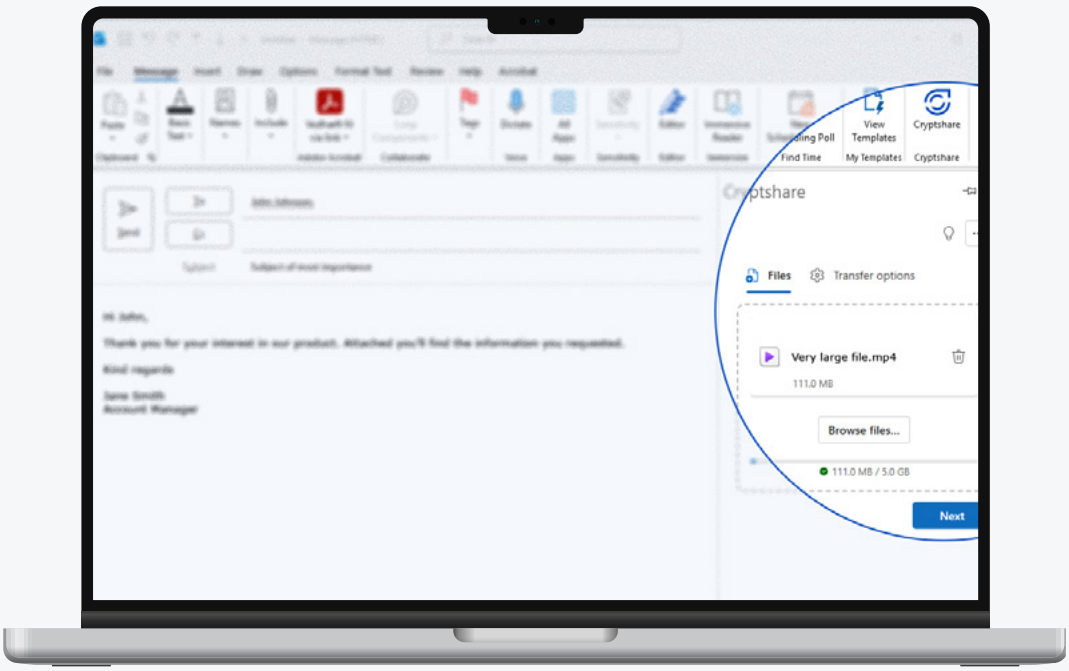
Skalierbarkeit
Das System kann mehrere Fälle parallel verarbeiten und auch größere Datenmengen bündeln.

Sicheres Datenhandling
Durch Cryptshare und API-basierte Prozesse bleibt die Kommunikation geschützt und nachvollziehbar.

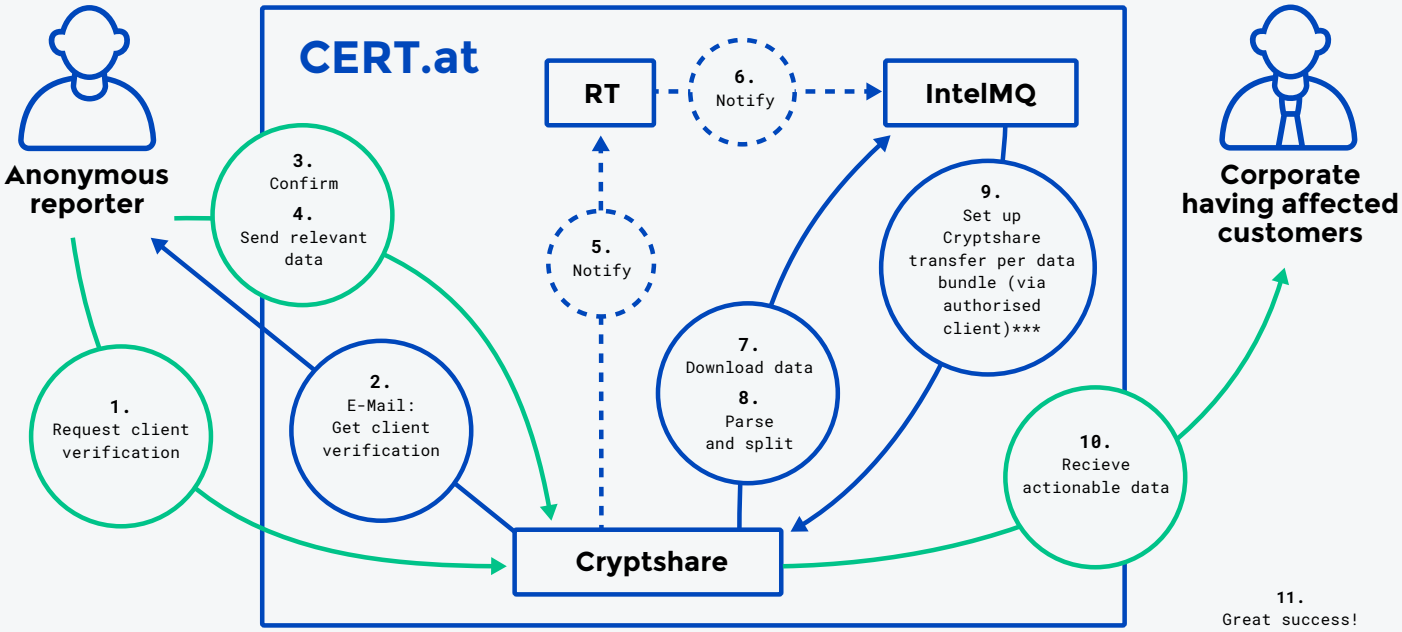
Transparenz
Erfolgreiche Übermittlungen werden lückenlos im System protokolliert.

Technische Besonderheiten

- Nutzung eines **Authorized Client-Mechanismus** zur automatisierten Datenübertragung
- Integration per **API-Schnittstellen** für flexible Anbindung von Finanzinstituten
- Möglichkeit zur **Bündelung kompromittierter IBANs** innerhalb von IntelMQ
- Aufbau eines **Lookup-Systems**, das die Zuordnung zu betroffenen Instituten ermöglicht



POINTSHARP



Erfolgsfaktor Vertrauen

Ein entscheidender Erfolgsfaktor ist die enge Zusammenarbeit zwischen **CERT.at und den Finanzdienstleistern**.

Nur durch gegenseitiges Vertrauen und klare Datenzuordnung konnte ein funktionierendes, schnelles Informationssystem aufgebaut werden.

Ergebnis

- Deutlich **schnellere Reaktionszeiten bei Phishing-Vorfällen**
- **Frühzeitige Information** betroffener Finanzinstitute
- Effektiver Beitrag zur **Reduktion von Finanzbetrugsschäden**
- Erfolgreicher Go-Live innerhalb kürzester Zeit

Ergebnis: Ein hochautomatisierter, sicherer und skalierbarer Prozess zur Bekämpfung von Phishing im Finanzbereich.

Ausblick

Die Lösung ist flexibel erweiterbar und bietet großes Potenzial für weitere Einsatzbereiche:

- Versicherungssektor
- Kryptoplattformen
- Fake-Shop-Erkennung
- Schutz bei Großveranstaltungen



Pointsharp ist ein europäisches Unternehmen für Cybersicherheit, dessen Produkte Firmenkunden die unkomplizierte Absicherung ihrer Daten, Identitäten und Zugänge ermöglichen. IT-Sicherheit muss einfach anzuwenden sein, daher ist es unsere Vision, allen Menschen den Zugang zu einem sicheren, modernen digitalen Arbeitsplatz zu ermöglichen. Wir bieten spezielle IAM-Lösungen, die auf anspruchsvollste Anforderungen jeglicher Art zugeschnitten sind.

Wir liefern in Europa hergestellte Cybersicherheitssoftware und -dienstleistungen für Kunden in aller Welt. Unsere Kunden sind häufig große Unternehmen, die ein besonders hohes Maß an Sicherheit und gesetzliche Auflagen erfüllen müssen, z.B. im Finanz-, Regierungs-, Industrie- und Verteidigungssektor.

Unser Hauptsitz befindet sich in Stockholm, Schweden, mit Niederlassungen in Deutschland, Dänemark, der Schweiz und den Niederlanden.

Pointsharp – security made easy

Kontaktieren Sie uns für weitere Informationen oder eine Demo

info@pointsharp.de

Neben der direkten Beziehung zwischen CERT.at und den Finanzinstituten fungiert die CONTINUM AG als vertrauenswürdiger langjähriger Servicepartner, der die Zusammenarbeit stabilisiert und professionalisiert.

Certified **Pointsharp** Partner

Continum

POINTSHARP