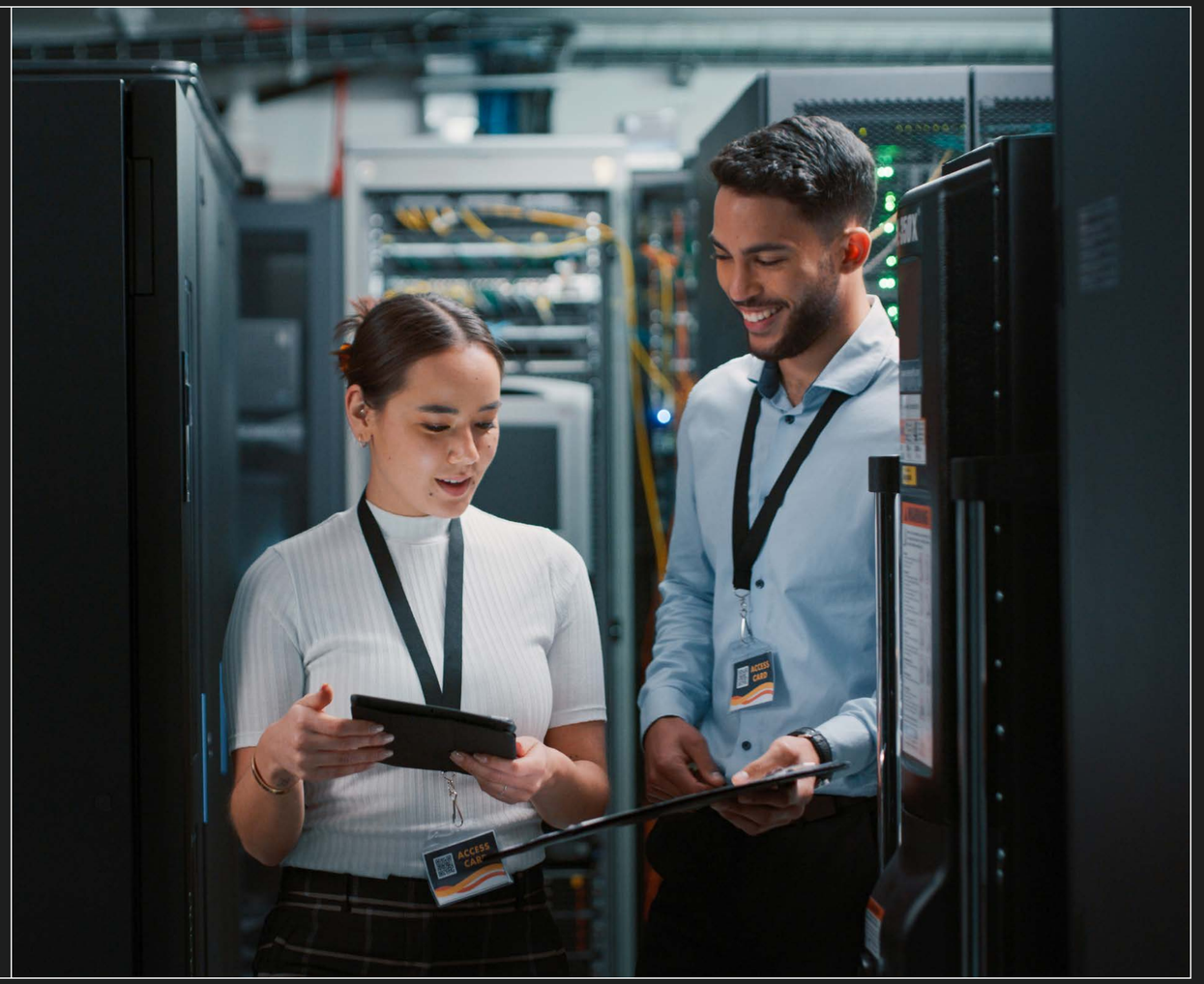
infopulse

Implementierung einer langfristigen Sicherheitsstrategie zum Schutz der Vermögenswerte von Infopulse und unseren Kunden in einem Krieg_

Zukunftssichere Sicherheitsstrategie für ultimativen Schutz

Kunde: Infopulse **Branche:** Software & Hi-Tech **Ort:** Ukraine

Experten: 2,300+ **Website:** www.infopulse.com



Über den Kunden

Infopulse, Teil des führenden nordischen Unternehmens für digitale Dienstleistungen Tietoevry, ist ein internationaler Anbieter von Dienstleistungen in den Bereichen Softwareentwicklung, Anwendungsmanagement, Cloud & Infrastruktur und Cybersicherheit für KMUs und Fortune-100-Unternehmen auf der ganzen Welt.

Anforderung

Wir von Infopulse sind der Meinung, dass unser Unternehmen die gleichen Grundsätze für alle internen Prozesse anwenden sollte, um qualitativ hochwertige, innovative und sichere Dienstleistungen zu erbringen. Wir sind bestrebt, eine robuste Infrastruktur aufzubauen und zu unterstützen, die den Anforderungen unserer Kunden in Bezug auf Sicherheit und Ausfallsicherheit gerecht wird und den Schutz der Datenbestände des Unternehmens gewährleistet. Um dies zu erreichen, hat Infopulse eine unternehmensweite Sicherheitsstrategie entwickelt und umgesetzt, die seit 2017 schrittweise verbessert und an die sich verändernde Bedrohungslage angepasst wird.

Für das Infopulse-Sicherheitsteam wurden folgende Ziele festgelegt:

- Gewährleistung des größtmöglichen Schutzes sensibler Daten und der Vermögenswerte der Kunden innerhalb des IT-Ökosystems von Infopulse.
- Erlangung eines umfassenden Verständnisses der neuen Arten von Cyberangriffen auf Unternehmen und staatliche Einrichtungen.
- Verbesserung der Infopulse-Infrastruktur mit fortschrittlichen Sicherheitstools und -ansätzen zur Abwehr moderner, raffinierterer Angriffe.
- Verfolgung eines proaktiven Ansatzes für die Cybersicherheit, um rechtzeitig auf erkannte Bedrohungen und Schwachstellen reagieren zu können.
- Regelmäßige Bewertung und Prüfung des Zustands des Sicherheitsbereichs des Unternehmens.
- Gestaltung und Verbesserung von Prozessen und Abläufen bis zur Perfektion für das Infopulse-Cybersicherheitsteam.
- Gewährleistung eines 360-Grad-Überblicks über die Sicherheitslandschaft des Unternehmens.

Lösung

Die Umsetzung der Sicherheitsstrategie von Infopulse war eng mit den Ereignissen verwoben, die im Laufe der Jahre eintraten und neue Kapitel in der Entwicklung der Bedrohungslandschaft darstellten. Unsere Experten haben auf die Ereignisse so reagiert, dass diesen neuen Bedrohungen und den entsprechenden Ansätzen wirksam begegnet werden kann.

2017-2021

Das Jahr 2017 ist berühmt-berüchtigt für die weltweite Verbreitung der NotPetya-Malware, die vor allem Organisationen in der Ukraine angriff. Damit wurde die Priorität auf die Abwehr groß angelegter zerstörerischer Angriffe und die Stärkung unserer Sicherheitsposition erhöht. Das Infopulse-Sicherheitsteam reagierte wie folgt:

- Implementierung eines QRadar SIEM-Systems. Die Lösung wurde über mehrere Jahre hinweg feinabgestimmt und mit neuen Regeln angereichert.
- In Anbetracht der neuen Arten von Angriffen arbeitete das Team an Ansätzen, die die Chancen eines erfolgreichen Angriffs deutlich verringern sollten.
- Verbesserte Segmentierung des Unternehmensnetzes durch eine zusätzliche interne Firewall und einen geschützten Jump-Host zur Verwaltung der Unternehmenssysteme.
- Verstärkte Zusammenarbeit mit dem internen IT-Team, um die Bemühungen um eine hohe Sicherheit für die eingeführten Dienste abzustimmen.
- Übernahme bewährter Verfahren zur sicheren Verwaltung von Unternehmenssystemen.
- In Zusammenarbeit mit Microsoft stellte Infopulse erfolgreich auf die Sicherheitslösungen der nächsten Generation um:
  - Als die Pandemie und später der Krieg die etablierten Prozesse störten, ermöglichte das Cloud-Hosting eine umfassende Unterstützung der Infopulse-Experten während des Umzugs und bewahrte die erforderliche Kontrolle über Arbeitsplätze und Unternehmensdaten. Es ermöglichte auch einzigartige Dienste, die den Sicherheitsbedenken der Kunden Rechnung trugen, wie z. B. die Remote-Datenlöschung.
  - Die Infopulse-Unternehmensdienste, einschließlich einer Microsoft 365-Suite, wurden in eine geschützte Cloud-Konfiguration migriert. Das gesamte Unternehmen ist nun durch einen der fortschrittlichsten Sicherheitskomplexe von Microsoft abgedeckt.
- Konzeption und Durchführung einer unternehmensweiten Sicherheitskampagne mit einem Online-Phishing-Simulator, der freundlicherweise von unserer Muttergesellschaft Tietoevry zur Verfügung gestellt wurde.
- Einleitung der nächsten Stufe zur Verbesserung des Reifegrads der Sicherheitsprozesse:
  - Formalisierung zahlreicher Sicherheitsprozesse, z.B. Incident Management, Vulnerability Management, Security Event Management, etc.
  - Entwicklung von Kriterien zur Messung der Effektivität und Leistung des Teams auf der Grundlage der Analyse der bestehenden Aktivitäten.

- Dies ermöglichte ein schnelles, effizientes und gut koordiniertes Arbeiten innerhalb des Teams, als der Krieg ausbrach.

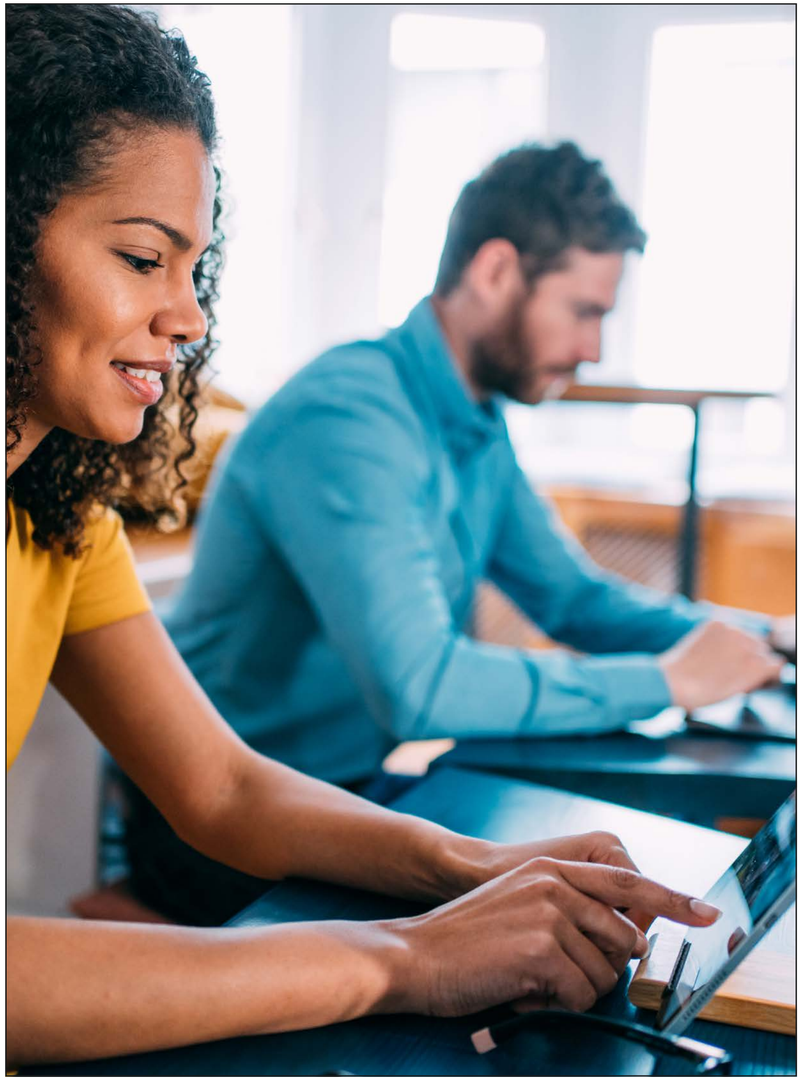
- Formalisierung und Konfiguration des Prozesses zur Verwaltung von Schwachstellen, um Schwachstellen in IT-Diensten rechtzeitig zu entdecken und in Zusammenarbeit mit dem IT-Team zu beseitigen:
  - Erzielung eines minimalen Schwachstellenprofils.
  - Im Dezember 2021 wurde das Schwachstellenmanagementsystem in die Cloud migriert, was eine schnelle und unkomplizierte Migration auf die EU-Plattform ermöglichte.

Januar 2022 “Letzte Vorbereitungen”

Ein Cyberangriff auf ukrainische Unternehmens- und Regierungswebseiten im Januar 2022 markierte den Beginn des Cyberkriegs, der sich im Hintergrund abspielte.

Im Rahmen seines Geschäftskontinuitätsplans entwickelte Infopulse eine Sicherheitsstrategie, um potenziellen Angriffen entgegenzuwirken und sich auf den bevorstehenden Krieg vorzubereiten:

- Treffen mit Tietoevry, unserer Muttergesellschaft, um die Anstrengungen abzustimmen und einschlägige Erfahrungen auszutauschen.
- Umfassendere Tests des Backup-Rechenzentrums in der EU.
- Umfassende Analyse von groß angelegten Cyberangriffen im Rahmen des Cyberkriegs.
- Der Aktionsplan für die Notfallsicherheit, der die wichtigsten Abläufe sicherstellen soll, wurde in den Mittelpunkt gestellt:
  - Verbesserter Schutz von Endpunkten und externen Webdiensten.
  - Migration der technischen Sicherheitslösungen in das EU-Rechenzentrum.
  - Identifizierung von Cybersicherheitsrisiken für Projekte, die für kritische Infrastrukturen arbeiten.
  - Abgestimmte zusätzliche Richtlinien für die Cloud-Sicherheit.
- Vorbereitung von Reservekommunikationskanälen, wie z. B. Satellitenverbindungen.



Februar-April 2022 “Wirksame Antwort”

Als Russland am 24. Februar in die Ukraine einmarschierte und einen grausamen Krieg begann, fand dieser sowohl auf der physischen als auch auf der digitalen Ebene statt. Viele ukrainische Standorte wurden angegriffen, was darauf hindeutete, dass es höchste Zeit war, einen neuen Ansatz und einen neuen Sicherheitsplan zu verabschieden, um dem ausbrechenden Chaos trotzen zu können:

- Infopulse erließ ein Verbot, wesentliche Änderungen vorzunehmen, mit Ausnahme von kritischen Aktivitäten für die IT- und Sicherheitsinfrastruktur.
- Verlagerung der Sicherheitslösungen in das EU-Rechenzentrum.
- Überarbeitung der laufenden Aktivitäten und Konzentration auf die wichtigsten Maßnahmen:
  - Umgang mit sicherheitsrelevanten Ereignissen
  - Analyse der Risikostandorte
  - Sperren von Unternehmenskonten auf Geräten an Risikostandorten.
- Unterstützung der sicheren Entwicklung der Anwendung “Infopulse Connect” zur effizienten Erfassung der erforderlichen Daten von allen Fachkräften des Unternehmens.
- Erstellung von Sensibilisierungsempfehlungen für die Fachkräfte, um sie vor Phishing-Angriffen zu warnen.
- Unterstützung einer regelmäßigen und umfassenden Kommunikation mit Kunden und Tietoevry über die Sicherheit unserer Mitarbeiter und den Schutz von Ausrüstung und Informationen.
- Ermöglichung der Notverlegung von Infopulsern und deren Familien, Ausrüstung und Sachgütern.
- Schutz von Büroräumen an gefährdeten Standorten und Vorbereitung weiterer Büroräume auf mögliche Schutzmaßnahmen.
- Evakuierung von Geräten aus dem Kiewer Rechenzentrum an einen sicheren Ort auf die effektivste und zuverlässigste Weise.
- Minimierung des Angriffsrisikos durch Abschalten von Diensten, die potenziell angegriffen werden könnten und im Moment nicht benötigt werden.
- Evacuated equipment from the Kyiv data center to a safe location in the most effective and reliable way.
- Minimized the perimeter for attacks by turning off services that could be potentially attacked and were not required at the moment.

Technologien

- **IBM QRadar SIEM**
- **Microsoft 365**
- **Cloud-Sicherheitslösungen**
- **Anti-Phishing-Lösungen**
- **WAF (Web Application Firewall)**
- **Azure AD Identity Protection**
- **EDR (Endpoint Detection and Response)**
- **SOC**

Ergebnis

Durch eine konsequente und gut durchdachte Sicherheitsstrategie erhielt Infopulse ein noch nie dagewesenes Maß an Schutz. Dank des proaktiven Ansatzes und der fundierten Entscheidungsfindung überstand Infopulse die gefährlichen Zeiten mit wenig bis gar keinem Schaden durch Cyberattacken. Hier ist unser Einsatz und Erfolg in Zahlen:

Geschäftskontinuität

- **Mehr als 30** Informationsmaterialien für Kunden über Servicekontinuität und Cybersicherheit erstellt.
- **Mehr als 20** Einsätze zur Umsiedlung und Evakuierung von Menschen und Ausrüstung durchgeführt.
- **Mehr als 270** Fachkräften des Unternehmens mit Hilfe des Relocation-Teams transportiert.
- Umzug von **2** Archiven mit physischer Dokumentation mit einem Gesamtvolumen von **3** Kubikmetern (**106** Kubikfuß).
- **Mehr als 60** Vorgänge über den Standort von Fachleuten in Risikogebieten wurden bearbeitet.

Unternehmenssicherheit

- **5** landesweite Cyberangriffe analysiert.
- **Mehr als 800** Phishing-E-Mails blockiert.
- Der Schutz von externen Webdiensten wurde um **110%** erweitert.
- **3** neue Cybersicherheitskontrollen wurden eingeführt.
- Verstärkte Implementierung von **5** Informationsdiensten unter dem Gesichtspunkt der Sicherheit.
- **100%**ige Abdeckung der Informationssysteme des Unternehmens mit einem effektiven Schwachstellenmanagementprozess.
- Aktualisierung von ca. **260** Verbindungen der Systeme zur Überwachung von Sicherheitsereignissen.
- **40%** mehr Cybersecurity-Ereignisse und -Vorfälle verarbeitet als in Friedenszeiten.
- **5** Vorfälle im Bereich der Informationssicherheit wurden bearbeitet.
- **6** spezielle Sicherheitsankündigungen wurden veröffentlicht.

Über Infopulse

Infopulse, Teil des führenden nordischen, digitalen Dienstleistungs-Unternehmens Tietoevry, ist ein internationaler Anbieter von Dienstleistungen in den Bereichen Software-F&E, Anwendungsmanagement, Cloud- und IT-Betrieb sowie Cybersicherheit für KMUs und Fortune 100 Unternehmen auf der ganzen Welt. Das in 1991 gegründete Unternehmen verfügt über ein Team von über 2,300 Fachleuten und ist weltweit in 7 Ländern - in Europa sowie in Nord-, Mittel- und Südamerika - vertreten.

Infopulse genießt das Vertrauen vieler etablierter Marken wie BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Offshore Norge, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group und vieler anderer.

Für weitere Informationen besuchen Sie bitte **www.infopulse.com/de**

Kontaktieren sie uns:

PL +48 (663) 248-737

DE +49 (69) 505-060-4719

US +1 (888) 339-75-56

UK +44 (8455) 280-080

UA +38 (044) 585-25-00

BG +359 (876) 92-30-90

BR +55 (21) 99298-3389

info@infopulse.com