GOVDIGITAL

Malware Information Sharing als gemeinsamer Ansatz für höheren Schutz

Uwe Schwarz | govdigital eG

22.04.2024

Agenda:

- Govdigital – Kollaborative Basis für öffentliche IT
- Aktuelle Cybersicherheitslage
- Umgang mit Bedrohungen und Bedrohungsinformationen
- Ein gemeinsamer Service für die öffentliche Verwaltung

Kollaborative Basis für die öffentliche IT

govdigital ist ein bundesweit ausgerichtetes öffentliches Unternehmen in der Rechtsform einer Genossenschaft. Ziel ist es, sichere und zuverlässige digitale Infrastrukturen für die Aufgaben der Verwaltung und der Daseinsvorsorge zu schaffen.

Unsere 28 Mitglieder sind öffentliche IT-Dienstleister aller drei Ebenen des föderalen Staats, die sich mit hoher Verbindlichkeit zu einem gemeinsamen Engagement verpflichtet haben.

Wir sind eine Inhouse-Gesellschaft. Mitglieder der govdigital und ihre Träger können die govdigital inhouse beauftragen.

Die govdigital hat drei Geschäftsmodelle

MARKTPLATZ für EfA-Leistungen

CLOUD SERVICE PORTAL

Open CoDE

MISP Threat Sharing

kubernetes

Cooperation-as-a-Service

Wir ermöglichen

bundesweite Kooperationen und Zusammenarbeit über alle Verwaltungsebenen hinweg.

Plattformen

Wir organisieren

bedeutende Plattformen der öffentlichen Verwaltung, bauen sie mit unseren Mitgliedern auf und steuern den Betrieb.

Genossenschafts-Services

Wir entwickeln

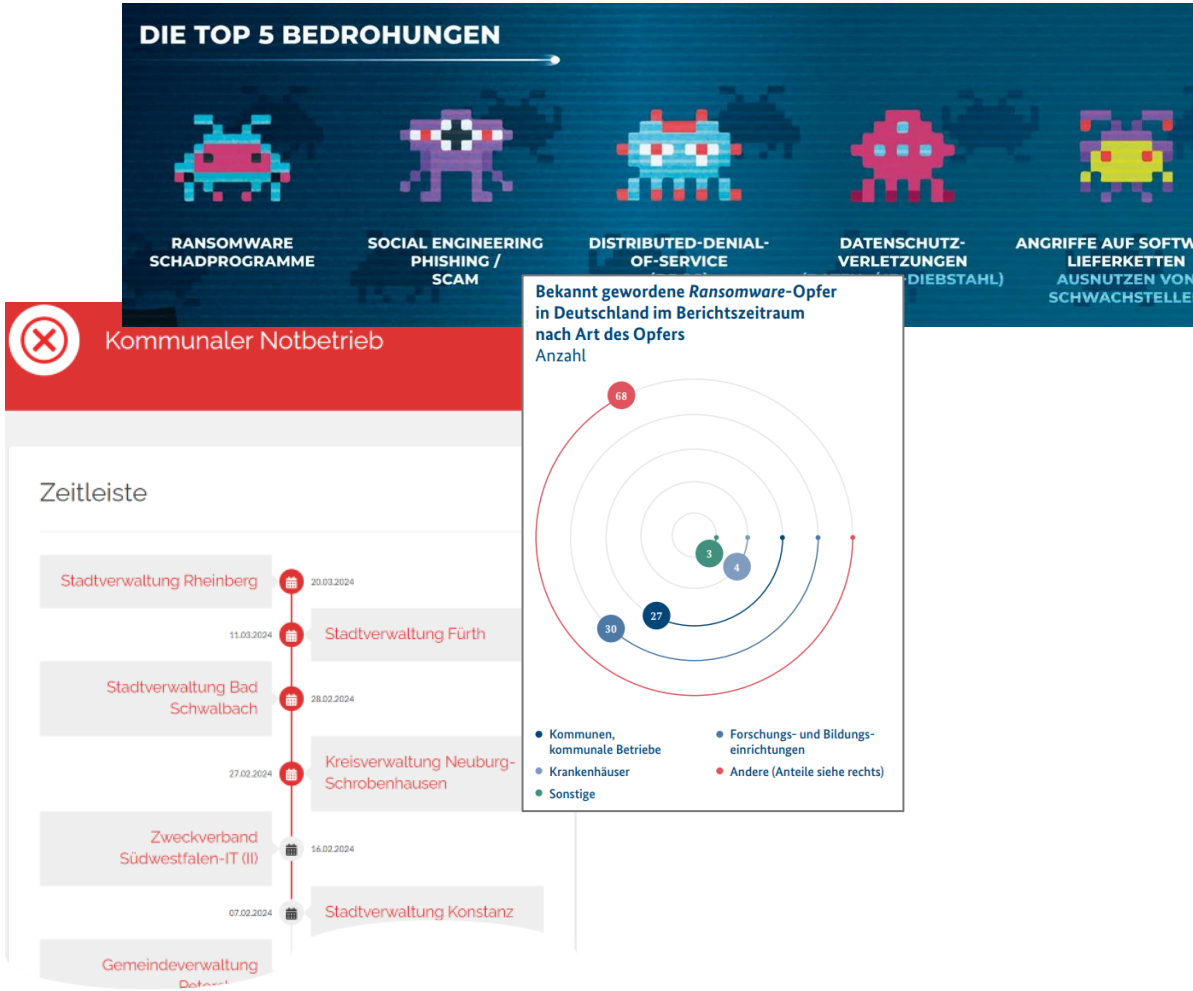
Lösungen mit und für unsere Mitglieder und setzen sie gemeinsam wirtschaftlich um.

Die große Reichweite der 28 Mitglieder ermöglicht Inhouse-Austausch zwischen Bund, allen Bundesländern und rund **85 Prozent aller kommunalen Gebietskörperschaften** in Deutschland.

Deutschland belegt einen Spitzenplatz in der Liste der europäischen Angriffsziele**

- 206 Milliarden Euro Schaden für deutsche Unternehmen in 2023 (Bitkom) - drei Mal in Folge über 200 Milliarden €!
- Stetig wachsende Zahl von Schwachstellen in Softwareprodukten – 70 Schwachstellen (weltweit täglich), 15% kritisch
- Professionalisierung und Spezialisierung der Cyberkriminalität*
- Zunehmende Investitionen und die Bereitschaft für mehr Cybersicherheit vs. Fachkräftemangel**
- Cyberkriminelle nehmen zunehmend den Weg des geringsten Widerstandes

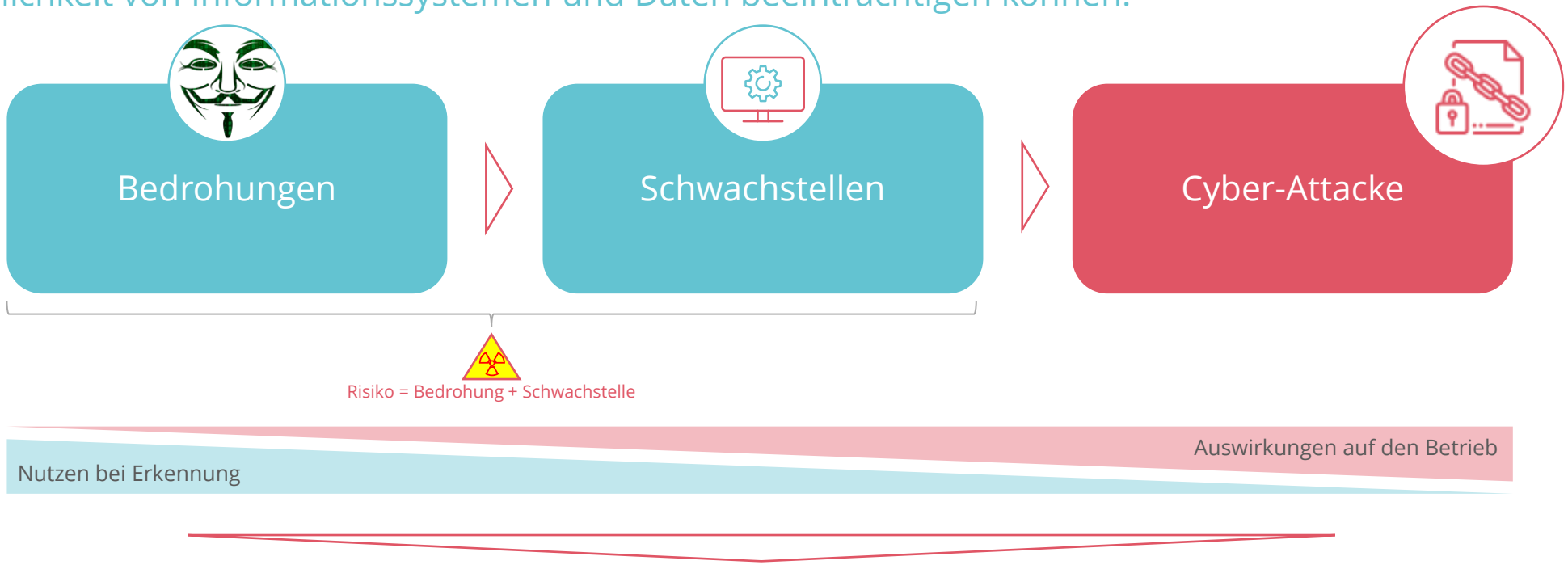
Cyber-Resilienz steigern



Quelle: *BSI-Lagebericht 2023; **2024 Cyber-Security Report Schwarz Gruppe

Handeln bevor es weh tut!

Bedrohungen in der Cybersicherheit fungieren als potenzielle Schadensquellen, die die Integrität, Verfügbarkeit und Vertraulichkeit von Informationssystemen und Daten beeinträchtigen können.



Frühzeitig relevante Bedrohungen erkennen und automatisiert dagegen vorgehen.

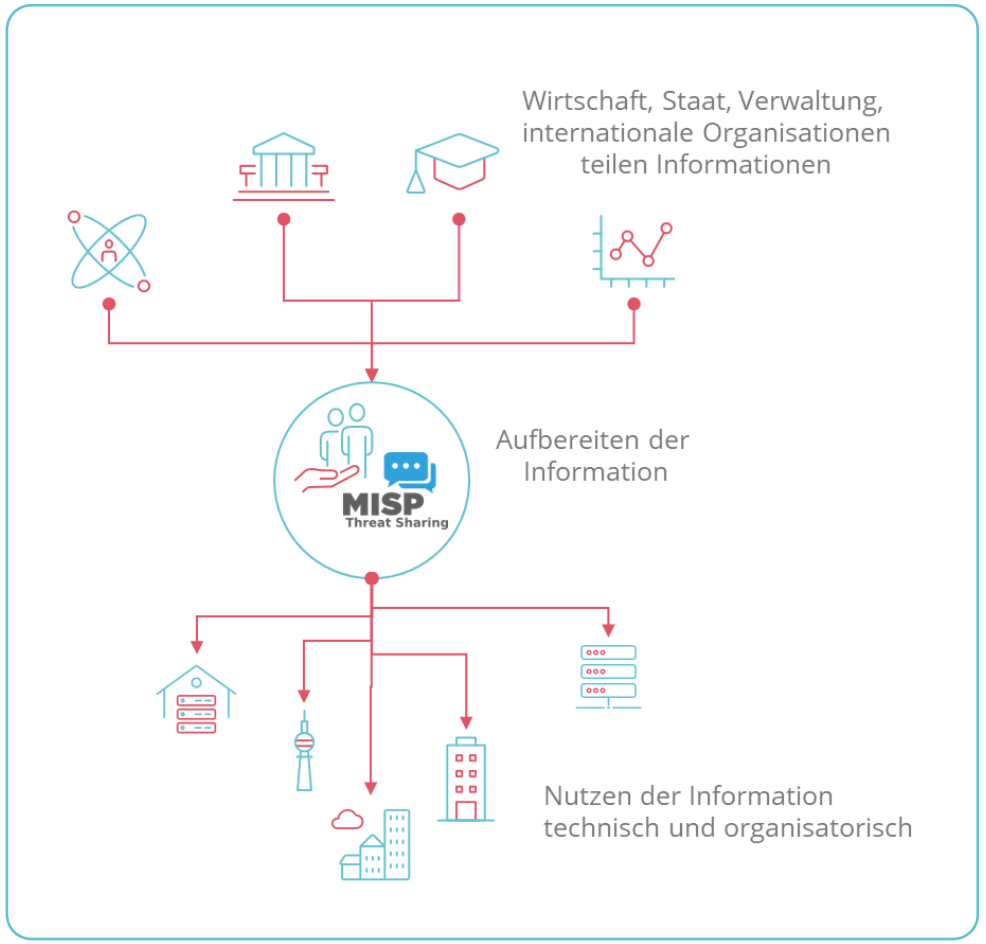
Bedeutung von Malware Information Sharing in der Cybersicherheit

Austausch von Informationen, Analysen und Echtzeit-Daten über Malware, Cyberangriffe und Schwachstellen

- Austausch erfolgt zwischen verschiedenen Organisationen und Einrichtungen – Wirtschaft, Staat, Verwaltung, internationale Organisationen
  - Technische Details,
  - Indikatoren für Kompromittierungen (IoCs),
  - Taktiken, Techniken und Verfahren (TTPs) von Angreifern
  - Abwehr- und Milderungsstrategien

- Die Rolle von Malware Information Sharing:
  - Frühzeitige Erkennung
  - Verbesserte Abwehrmaßnahmen
  - Effizienzsteigerung
  - Förderung der Zusammenarbeit
  - Bildung eines kollektiven Wissens

Informationen teilen erfordert Austausch



Herausforderungen durch das Teilen von Informationen müssen adressiert werden.

Datenschutz und Vertraulichkeit	„4-Augen-Prinzip“ durch Redaktion
Standardisierung der Formate	Gemeinsame Taxonomie
Effektive Kommunikation	Moderierte Kommunikation, Sharing Calls
Technologische Kompatibilität	Relevanz ermitteln
Ressourcen und Kapazität	Gemeinschaftlicher Betrieb und Automatisierung
Etablieren von Vertrauen	Feste Basis etablieren – Sharing Policy

Gemeinsamer Ansatz für höheren Schutz

Operationalisieren von Bedrohungsinformation

Wesentliche Elemente:

- **Sharing Policy** vereinbart.
- Regelmäßige **Sharing Calls** zum Teilen von Information, Erfahrung und Erkenntnis.
- Gemeinsame **technische Plattform** ermöglicht schnelles Handeln, die **Taxonomie** ist definiert.
- **Redaktion** ermöglicht Steigerung der **Relevanz** und Verbesserung der **technischen Qualität**; geringe Anzahl „False Positives“.
- **Rückkopplung** für die technische Integration eigener Erkenntnis – insbesondere über Fachverfahren.

Service verfügbar seit 01/2024

Einzigartige Informationen

- **Eigene Sensorik** und dadurch einzigartige Informationen
- Einbettung in **enge Kooperation** (Sharing Calls, Feedback)
- Schwachstellen von **Fachverfahren**

Passende Angebote für Einsteiger und Experten

- **Erste Erfahrungen sammeln** (Sharing Calls) und Reports
- Zugriff auf technische Information, **eigene Erkenntnisse einfach operationalisieren**

Starke Partnerschaft mit der DCSO

- **Expertise** deutscher Großkonzerne
- Vertrauensvolle **Partnerschaft** mit BSI, BND und BfV
- Netzwerk auch in **Krisensituationen**

Maßgeschneiderter genossenschaftlicher Service

- **Hohe Relevanz** der Informationen für die öffentliche Verwaltung / IT-Dienstleister
- **Reduktion lokaler Aufwände** durch redaktionelle Unterstützung
- **Keine Konkurrenz** um knappes, hochspezialisiertes Personal

Passende Angebote für Einsteiger und Experten

Der Service richtet sich an Organisationen, denen gegenüber die govdigital „inhouse-fähig“ ist.

	Bronze (Basic)	**Silber** (Essential)	**Gold** (Advanced)
TI-Content	Weekly / AdHoc Report	Weekly / AdHoc Report Tech. Indikatoren	Weekly / AdHoc Report Tech. Indikatoren
Redaktion	Sharing Call	Sharing Call Rücklauf / Mitglieder Wünsche	Sharing Call Rücklauf / Mitglieder Wünsche
Zentrale MISP	✗	✓	n/a
Eigene MISP	✗	✗	✓

Einzelaspekte zur Prüfung an der Teilnahme des Services:

1. Kann der IT-Betrieb die Absicherung verbessern?
2. Können die Informationen die Resilienz und Sicherheit der eigenen Systeme beeinflussen?
3. Ist das Risikomanagement der IT oder der Informationssicherheitsrisiken in eigener Verantwortung?
4. Können eigene Erkenntnisse und Einschätzungen die anderen Teilnehmer befähigen, davon zu profitieren?

Das gemeinschaftliche Malware Information Sharing zeichnet sich durch spezifische Alleinstellungsmerkmale für die öffentliche Verwaltung aus.

- Spezifische / Relevante Bedrohungs-information für die ÖV
- Redaktionelle Unterstützung
- Schwachstellen von Fachverfahren
- Gemeinschaftliche Leistung adressiert Fachkräftemangel
- Hohe Qualität fördert Automatisierung
- Vertrauensvolles Netzwerk
- Hohe Expertise

Zusammenfassung

- Bedrohungslage wächst und ist für einzelne Organisationen kaum überschaubar
- Individuelle Bedrohungen erkennen - Frühzeitiges Agieren steigert die Cyber-Resilienz
- Spezifische Informationen gleichgesinnter verhindern Angriffe - Relevanz
- Gemeinsames Handeln und Automatisierung helfen bei zunehmendem Fachkräftemangel

Die govdigital stellt vertrauensvolle Basis bereit.

Das Security-Services Angebot wächst stetig

Business Continuity Management

ekom21

GOVDIGITAL

Business Continuity Management

Dreitägiges Seminar für Kommunen auf Basis BSI-Standard 200-4

Hochwasser, Blackout, Cyberangriffe – die Ursachen für Ausfälle des Verwaltungsbetriebs können vielfältig sein. Bei solchen Schadensereignissen gilt es, schnellstmöglich einen Überblick zu gewinnen, um Folgeschäden abzuwenden und besonders zeitkritische Geschäftsprozesse fortzuführen.

Um eine verlässliche Absicherung des Verwaltungsbetriebs zu gewährleisten, liegt der besondere Fokus des Seminars auf der Anwendung des BSI-Standards 200-4 auf kommunale Bedarfe. Ziel ist der Aufbau eines Business-Continuity-Management-Systems (BCMS) für die Kommunalverwaltung.

Dabei werden die Arbeit eines Krisenstabs methodisch organisiert, der Verwaltungsbetrieb auf zeitkritische Vorgänge und Geschäftsprozesse hin durchleuchtet und diese nach genaueren Analysen durch Strategien, Maßnahmen und Notfallpläne präventiv oder reaktiv abgesichert.

Kontakt
Uwe Schwarz
CISO / Leiter Geschäftsfeld Cybersicherheit
E-Mail: uwe.schwarz@govdigital.de

Dreitägiger Workshop zur Planung und Umsetzung des BSI-Standards 200-4

Das Training ist für Personen entwickelt, die BCM in ihrer Institution ganz oder teilweise organisatorisch zu verantworten haben oder an dessen Umsetzung mitwirken.

Organisation und Durchführung: govdigital eG gemeinsam mit dem hessischen kummunalen IT-Dienstleister ekom21 - KGRZ Hessen

Termine und Anmeldung:
https://www.ekom21.de/bcm-schulung

Inhalte u.a.:
- Aufbau und Planung eines BCM
- Aufbau der Leitlinie
- Aufbau des Notfallvorsorgekonzepts
- BCM-Risikoanalyse
- Üben und Testen im BCM

govdigital eG ● www.govdigital.de

Phishing-Simulation

GOVDIGITAL

Phishing-Simulation

Phishing bleibt ein Dauerbrenner unter den zehn größten Angriffstrends.

Wir helfen Ihnen, Ihre Mitarbeitenden zu trainieren, schadhafte E-Mails zu erkennen. Für mehr Sensibilität und Aufmerksamkeit erhalten Sie bis zu zwölf Simulationen in mehreren Intervallen und „Schwierigkeitsstufen".

Die Gefahr gefälschter E-Mails ist ungebrochen. Täuschend echte Nachrichten werden von unsicheren Quellen versendet und fordern Mitarbeitende auf, sich an gefälschten Web-Seiten anzumelden oder maliziöse Links zu klicken. Angriffe dieser Art werden zunehmend besser und gezielter.

Diese E-Mails haben häufig einen bedrohlichen Unterton, der zum schnellen Handeln verleiten soll. Häufig wird suggeriert, so einen vermeintlichen Fehler noch korrigieren oder einer dringlichen Anforderung nachkommen zu können. In Wirklichkeit versuchen Kriminelle, sich Zugang zu Systemen zu verschaffen oder Schadsoftware einzuschleusen.

Mit Phishing-Simulation stellt Ihnen govdigital eG zusammen mit der Komm.ONE AöR eine vertrauenswürdige Awareness-Maßnahme zur Verfügung.

Kontakt
Uwe Schwarz
CISO / Leiter Geschäftsfeld Cybersicherheit
Mobil: +49 175 / 413 7242
E-Mail: uwe.schwarz@govdigital.de

Unser Angebot

Awareness-Maßnahme zur Bekämpfung von Phishing-Attacken, die mit folgendem Angebot individuell angepasst werden kann.

Initiale Sensibilisierung durch eine Einmalaktion („Single Shot")

Entwicklung erhöhter Aufmerksamkeit durch regelmäßige Simulationen und verschiedenen Schwierigkeitsstufen.

Begleitende Aktivitäten: Aufsteller, Plakate, Post-its

govdigital eG ● www.govdigital.de

Malware Information Sharing

GOVDIGITAL

Malware Information Sharing (MIS)

Steigerung der Cyber-Resilienz durch geteilte Informationsbasis

Cybersicherheit ist eine Frage von Expertise – und Geschwindigkeit. Je eher relevante Informationen in die eigene Verteidigung einfließen, desto besser die Chance zur Abwehr. govdigital bietet eine gemeinsame Plattform, die qualitativ einzigartige Informationen und passende Services bereitstellt.

Angriffserkennung und Angriffsvermeidung: Das Malware Information Sharing (MIS) der govdigital ermöglicht es, Bedrohungen durch private, kommerziell organisierte oder staatliche Akteure zu erkennen, zu sammeln, aufzubereiten und automatisiert in Prozesse zu integrieren.

Durch die gemeinsame redaktionelle Aufarbeitung und Qualitätssicherung ist das MIS ein wesentlicher Bestandteil der automatisierten technischen Nachnutzung der Bedrohungsinformationen. Der Service ermöglicht es, Aufwände zu reduzieren, damit sich Security-Experten vor Ort auf ihre Aufgaben und Maßnahmen konzentrieren können. Das MIS für öffentliche Verwaltungen ist in der Lage, spezifische Daten etwa aus Fachverfahren einzuschließen – Informationen, die am Markt so nicht verfügbar sind.

Kontakt
Uwe Schwarz
CISO / Leiter Geschäftsfeld Cybersicherheit
E-Mail: uwe.schwarz@govdigital.de

Malware Information Sharing

Einzigartige Informationen
- Eigene Sensorik, einzigartige Informationen
- Hohe Qualität, einfache Nachnutzung
- Einbettung in enge Kooperation (Sharing Calls, Feedback

Passende Angebote
- Erste Erfahrungen sammeln (Sharing Calls) und Reports nutzen
- Technische Information und eigene Erkenntnisse einfach operationalisieren

Starke Partnerschaft (DCSO)
- Expertise deutscher Großkonzerne durch Kooperation mit der Deutschen Cyber-Sicherheitsorganisation (DCSO)
- Vertrauensvolle Partnerschaft mit BSI, BND und BfV
- Netzwerk auch in Krisensituationen

Maßgeschneiderter Service
- Hohe Relevanz der Informationen für die öffentliche Verwaltung / IT-Dienstleister
- Reduktion lokaler Aufwände durch redaktionelle Unterstützung
- Keine Konkurrenz um knappes, hochspezialisiertes Personal

govdigital eG ● www.govdigital.de

Das Security-Services Angebot wächst stetig

Business Continuity Management Phishing-Simulation Malware Information Sharing

Email: Uwe.Schwarz@govdigital.de
Tel: +49 175 413 7242