DataArt

Pyramide der Unternehmenssicherheit

Erstellt von:

Dmitry Vyrostkov Dmitry.Vyrostkov@dataart.com

Friedrich Stahl Friedrich.Stahl@dataart.com

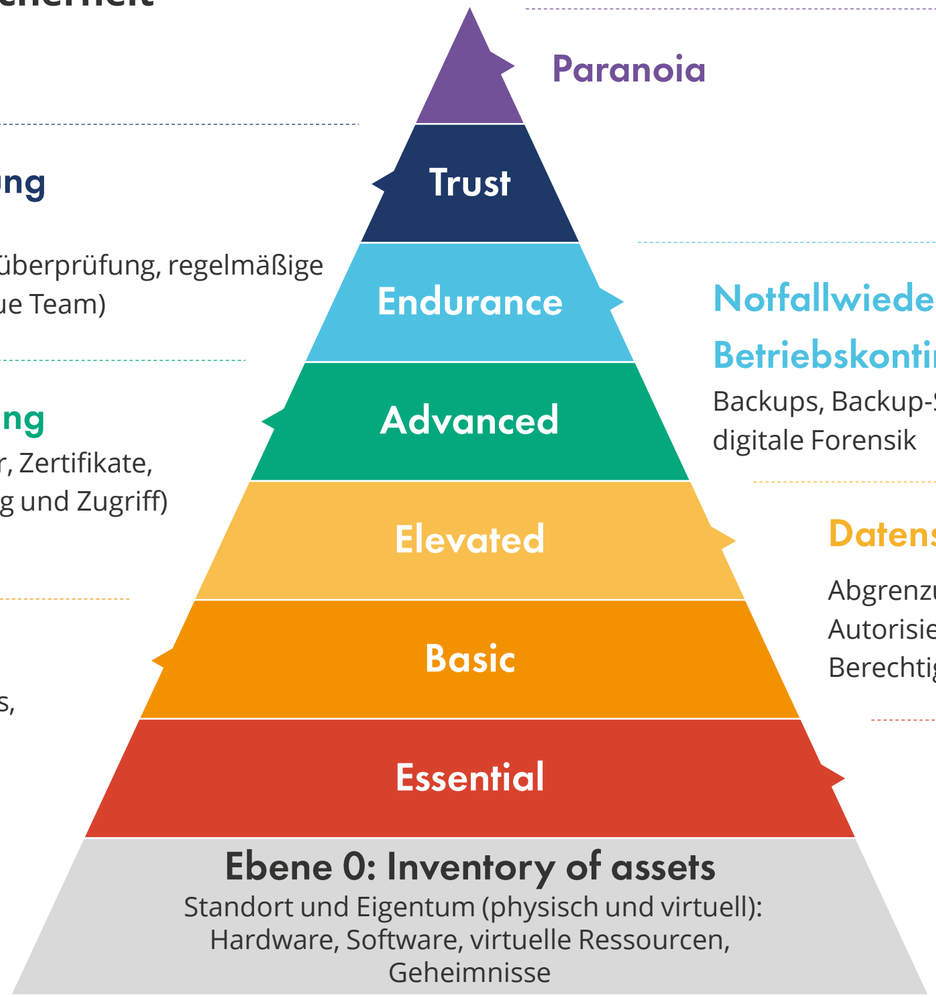
Sebastian Bucur Sebastian.Bucur@dataart.com

Sicherheit ist kein Zeitpunkt, sondern ein Prozess

7 Schutzebenen

DataArt

Pyramide der Unternehmenssicherheit



Ebene 7

Ebene 6

Hintergrundprüfung

Personal-Screening, Lieferkette/Lieferantenüberprüfung, regelmäßige Pentests (Red Team, Blue Team)

Ebene 5

Notfallwiederherstellung – Betriebskontinuität

Backups, Backup-Systeme, Notfallplan für Cybersicherheit, digitale Forensik

Ebene 4

Dokumentenklassifizierung

Secrets Management: Passwörter, Zertifikate, vertrauliche Dateien (Archivierung und Zugriff)

Ebene 3

Datenschutz während der Speicherung

Abgrenzung von Personal und Maschinen: Autorisierung, Zugangskontrolle (Rollen, Berechtigung), Datenverschlüsselung

Ebene 2

Perimeterschutz

Firewall, Eindringungserkennung, Antivirus, Authentifizierung (RFID-Zugang), Sicherheitsaudit (regelmäßig)

Ebene 1

Standardeinstellungen und Passwörter

Einstellungen, Passwörter, Schnittstellen, Konfigurationsdateien, Firewall, Passwort-Richtlinien und -Zertifikate

Ebene 0: Inventory of assets

Standort und Eigentum (physisch und virtuell): Hardware, Software, virtuelle Ressourcen, Geheimnisse

Sicherheitspyramide | Überblick

Warum 7 Ebenen?

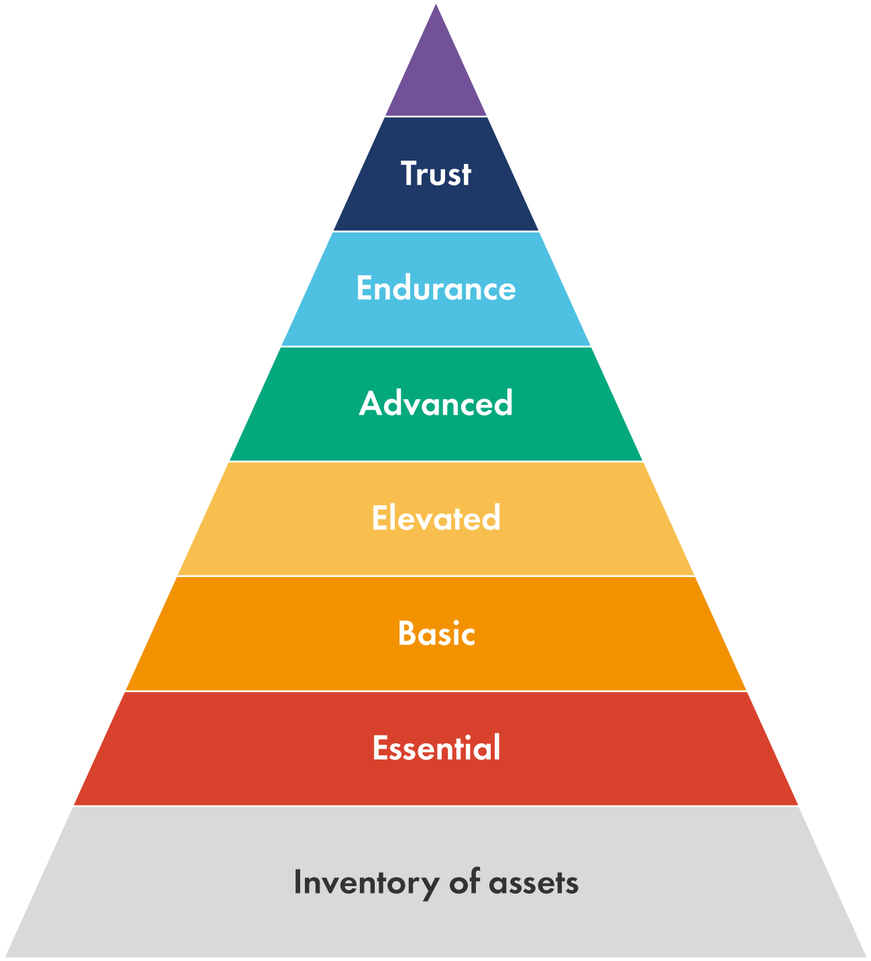
DataArt

Cybersicherheit ist ein weites Feld, und jedes Unternehmen hat ein anderes Sicherheitsniveau. Jede Ebene der Pyramide befasst sich mit einer bestimmten Gruppe von Bedrohungen und Risiken.

Im Sicherheitsbereich ist Prävention weitaus besser als Schadensbehebung. Je höher die Sicherheitsstandards eines Unternehmens sind, desto unwahrscheinlicher sind Konfrontationen mit Sicherheitsvorfällen, die sich drastisch auf das Geschäft auswirken würden.

Sicherheitsrisiken:

- Durchsickern vertraulicher Informationen
- Sicherheitsbruch
- Datenverlust, Datendiebstahl
- Rufschädigung
- Ransomware, Malware
- Nichteinhaltung (Bußgelder, Klagen)
- *und so weiter*



Jüngste Sicherheitsrisiken

DataArt

Social Engineering

Fahrlässigkeit der IT-Abteilung

Malware & Ransomware

Nichteinhaltung von Vorschriften

Gezielter Angriff

In 2018 und 2019:

facebook

50 Millionen Benutzerdaten exponiert. Bußgeld in Höhe von $1.6 Milliarden von der EU

Marriott

300 Millionen Kundendaten gestohlen. $500 Millionen Schadenersatz

BINANCE

7 000 Bitcoins gestohlen. $40 Millionen Schadenersatz

Google+

53 Millionen Benutzerdaten exponiert.

Google schließt endgültig den Service von G+

Capital One Bank

100 Millionen Kreditanträge exponiert.

Sicherheitspyramide |
Ebene für Ebene

Ebene 0. Inventory of assets (Bestandsverzeichnis)

DataArt

Unternehmen benutzen eine Vielzahl unterschiedlicher Software. Die Nachfrage nach noch mehr Anwendungen und Hardware läuft proportional zum Unternehmenswachstum. Den Überblick über all diese digitalen Assets zu behalten ist herausfordernd und äußerst wichtig.

Sie können nur die Assets beobachten, die Sie auch kennen.

Eine Bestandsaufnahme von Assets ist der erste Schritt, um Ihr Unternehmen vor böswilligen Angriffen von innen oder von außen zu schützen.

Lokalisieren Sie die Hardware

Server, Switches, Router, PC-Stationen, Laptops, Smartphones etc.

Lokalisieren Sie Geschäftsgeheimnisse

- Stellen Sie fest, wo Passwörter und Zertifikate gespeichert sind und wer Zugriff darauf hat.
- Bewahrung von Geheimnissen: kreieren, erneuern, entziehen, wechseln.

Lokalisieren Sie virtuelle Ressourcen

Virtuelle Laufwerke (Google, Microsoft, andere), Cloud Buckets, virtuelle Maschinen, API Gateways, Docker und Kubernetes Container.

Bestimmen Sie Verantwortlichkeiten

Die verantwortliche Person für jedes einzelne Element.

Ebene 1. Essential (erforderlich)

DataArt

Standardeinstellungen und Passwörter machen Angreifern das Leben sehr einfach. Scheinbar belanglos, bleibt dies eines der größten Sicherheitsrisiken für jedes Unternehmen, unabhängig von Größe und Art.

Nachdem alle Assets lokalisiert wurden, müssen Sie im nächsten Schritt alle Standardeinstellungen ändern:

Passwörter

Schnittstellen

Firewallregeln

Zertifikate

Einstellungen

Konfigurations-dateien

Passwort-Richtlinien

Es wird empfohlen, dass IT-Ingenieure von Fall zu Fall unnötige Komponenten deaktivieren und nicht unbedingt erforderliche Anwendungen deinstallieren. (z.B. muss auf dem Computer eines Buchhalters keine Eingabeaufforderung installiert sein – dies ist ein Sicherheitsrisiko).

Ebene 2. Basic (grundlegend)

DataArt

Perimeterschutz

Der Perimeterschutz muss sowohl im physischen als auch im virtuellen Bereich implementiert werden. Zutritt zu Büroräumen, in denen Computer und Netzwerkinfrastruktur vorhanden sind, muss eingeschränkt werden.

Firewall

- Nehmen Sie erweiterte Einstellungen vor
- Verwenden Sie eine virtuelle oder physische Anwendung (Verlassen Sie sich nicht auf die Firewall-Voreinstellungen des Betriebssystems)

Angriffserkennungssoftware

Sicherheitsprüfung und Audits

- Sicherheit ist ein Prozess und benötigt Pflege

Antivirus

- Richtig konfigurieren und regelmäßig aktualisieren.

Sicherheitsbewusstsein der Mitarbeiter schulen

Authentifizierung (RFID-Zugang), um Unbefugten den Zutritt zu verweigern

Ebene 3. Elevated (erweitert)

DataArt

Trennung der Aufgaben

Die tatsächliche Trennung muss auf Software-, Hardware- und Netzwerkebene erfolgen. Dies ist vielleicht nicht wirtschaftlich, aber es verbessert die Sicherheit und kann die Auswirkungen einer Sicherheitsverletzung begrenzen. Vermeiden Sie z.B. die Verwendung der gleichen Hardware für Webaufstellung, Datenbank und aktive Verzeichnisse. In einem solchen Fall hätte der Angreifer Zugriff auf alle Komponenten anstelle einer begrenzten Anzahl..

Trennung der Funktionen

Arbeitsaufgaben müssen so aufgeteilt und zugewiesen werden, dass einzelne Mitarbeiter und dedizierte Teams voneinander getrennt werden. Die Anzahl von berechtigten Personen, die Zugriff auf eine Plattform, ein Betriebssystem oder ein Gerät haben, solte begrenzt, bekannt und individuell gewährt werden.

IAAA Prinzip

- **I**dentifizierung
- **A**uthentifizierung
- **A**utorisierung
- **A**udit

Ebene 4. Advanced (fortgeschritten)

DataArt

Dokumentenklassifizierung

Dokumente müssen mindestens in 3 Kategorien eingeordnet werden: Öffentlich, Privat, Geschützt. Einschränkungen zum *Öffnen, Lesen, Kommentieren, Bearbeiten und Herunterladen* müssen basierend auf der Benutzerrolle definiert werden (Beispiel: Alle Mitarbeiter der C-Ebene können Finanzdokumente lesen).

Secrets Management

Passwörter

- Speichern Sie diese niemals in Klartext.
- Benutzen Sie 2FA oder MFA (Zwei-Faktor- oder Multi-Faktor-Authentifizierung).
- Verwenden Sie Passwortmanager oder Kenntworttresore.

Zertifikate

- Benutzen Sie wichtige Steurunginstrumente wie AWS KMS, Azure Key Vault oder HashiCorp Vault.

API-Schlüssel

- Codieren Sie diese niemals fest in Konfigurationsdateien oder im Quellcode.
- Verwenden Sie Verschleierungsmethoden

Ebene 5. Endurance (fortdauernd)

DataArt

Es gibt eine weitere Bedrohung, die weder durch starke Passwörter noch durch Verschlüsselung gemindert werden kann. Katastrophen wie Überschwemmungen, Erdbeben, schwerwiegende Hardwarefehler oder Sabotage können den Geschäftsbetrieb unterbrechen oder möglicherweise sogar zerstören. Dennoch gibt es Wege, sich vor solchen Bedrohungen zu schützen. Nicht indem versucht wird, diese zu vermeiden, sondern indem ein Plan zur Minimierung des Schadens und zur Verkürzung der Wiederherstellung erstellt wird. Verwenden Sie Folgendes:

Notfallkonzept

Backup-Systeme, Hardware, Stromgenerator, stellvertretender Internetdienstanbieter

Notfallplan zur Cybersicherheit

Datensicherung

Führen Sie Notfallübungen durch

Aktualisieren Sie die Pläne, falls sich die Infrastrukturkonfiguration ändert (Expansion, Fusion oder Übernahme eines anderen Unternehmens)

Digitale Forensik (Beweise sichern, Sicherheitslücken untersuchen/beseitigen/beheben)

Ebene 6. Trust (vertrauend)

DataArt

Hintergrundüberprüfung

Verwenden Sie Personal-Screening (Hintergrundüberprüfung), wenn Sie Mitarbeiter in Schlüsselpositionen beschäftigen oder diese Zugriff auf private Daten, Benutzerdaten, vertrauliche Dateien, wichtige Dokumente, Finanzinformationen usw. haben.

Überprüfungsprozess für Lieferanten und Verkäufer vor Vertragsabschluss. Fordern Sie diese gegebenenfalls dazu auf, ihre Sicherheitsstufe zu erhöhen.

Dark Web Scan. Verwenden Sie spezielle Systeme, die die Informationen im Deep Web durchsuchen, um festzustellen, ob Hacker im Besitz von Kreditkarten, Passwörtern oder sogar einer Liste von Benutzern und gestohlenen Berechtigungsnachweisen einer Firma sind.

Simulation gezielter Angriffe:

- Rotes Team (von außen)
- Blaues Team (von innen)

Ebene 7. Paranoia (paranoid)

DataArt

Diese zusätzliche Sicherheitsebene wird von regulären Unternehmen normalerweise nicht benötigt, wird selten eingesetzt und kann sehr teuer sein. **Besondere Sicherheitsmaßnahmen:**

Security Operation Center. E-Mail-Liste, spezielles Formular auf der Webseite oder im Intranet, in dem das Incident Response Team (Notfallteam) in Echtzeit helfen und auf Vorfälle reagieren kann.

Erkennen von Insider-Bedrohungen. Dies ist eine spezielle Stealth Software, die das Verhalten von Mitarbeitern analysiert, indem sie lernt, zwischen normalen und ungewöhnlichen Mustern zu unterscheiden. Das System kann Erkennungssignale setzen und die Verantwortlichen können Maßnahmen ergreifen, bevor eine interne Sicherheitslücke entsteht.

Biometrischer Zugang. Systeme, die Netzhautscanner, Stimmerkennung und Authentifizierung per Fingerabdruck beinhalten (müssen in Verbindung mit anderen Kontrollen durchgeführt werden, die für sich genommen weniger effektiv sind).

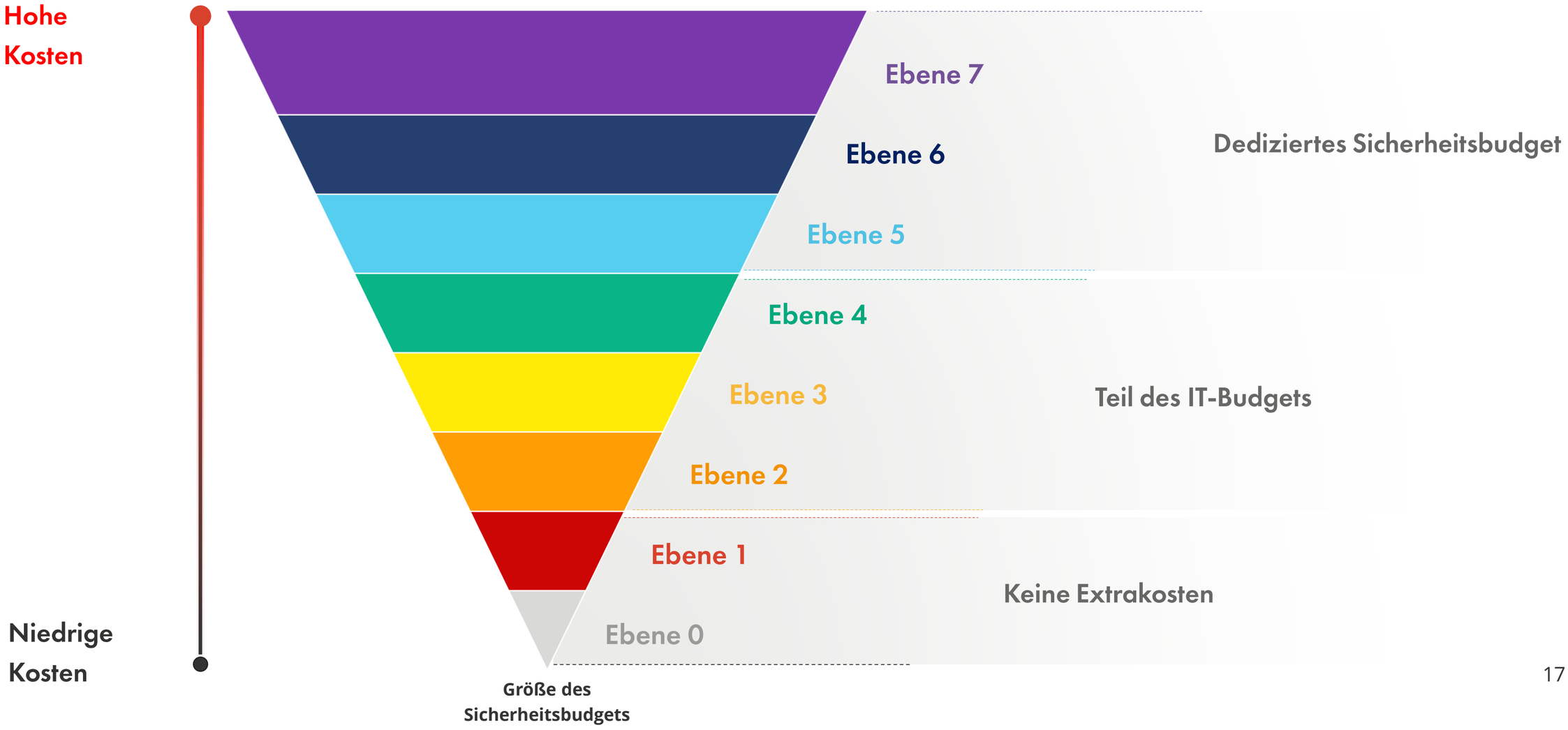
Sicherheitsüberprüfung kann für die Arbeit mit vertraulichen, geheimen und streng geheimen Informationen erforderlich sein. (Jedes Land hat unterschiedliche Ebenen und Normen).

Schulung zur Spionageabwehr zum Schutz des Personals vor Industriespionage. Schlüsselpersonen, die Zugang zu sehr wichtigen Informationen haben (Patente, Finanz- und Geschäftsgeheimnisse usw.), werden überwacht und auch geschützt, um zu verhindern, dass diese absichtlich oder gezwungenermaßen (durch Erpressung) vertrauliche Informationen an die Konkurrenz oder ausländische Unternehmen weitergeben.

Kosten für gute Sicherheit

Finanzplanung für Sicherheit

DataArt



Sicherheitsdienstleistungen | von DataArt

Unsere Dienstleistungen

DataArt

Penetrationstest

Cloud-Sicherheitsaudit

Codeüberprüfung

Social Engineering Test

Compliance Management

Sicherheitsgarantie

Sicherheitsberatung

Unsere Kunden

DataArt

skyscanner

ocado

Travelport

R.E.G. Regulatory Efficiency Gains

Tinkoff Bank

bondwave

monex EUROPE

Lindblad Expeditions | NATIONAL GEOGRAPHIC

artnet®

APPLE LEISURE GROUP

Bleiben Sie sicher & verbessern Sie Ihre Sicherheit!

Vielen Dank! Verschlüsseln Sie sicher!

DataArt

Dmitry Vyrostkov

Security & Software Expert

Dmitry.Vyrostkov@dataart.com

Friedrich Stahl

VP, Business Development

Sebastian.Bucur@dataart.com

Sebastian Bucur

Security Expert

Sebastian.Bucur@dataart.com

Zug
Schweiz

Alexander Makeyenkov
Managing Partner
+41 (0) 415 880 158
CH-Sales@dataart.com

München
Deutschland

Konstantin Kazin
Managing Director
+49 (89) 635 09 128
DE-Sales@dataart.com