Solution Set – Insider Threat Mitigation

Insider Threat:
Eine Gefahr welche einem Unternehmen bzw. einer Organisation daraus erwächst, dass eine Person die befugt ist (oder war) auf Systeme oder Daten zuzugreifen, durch böswillige oder unabsichtliche Handlungen Schaden verursachen könnte.

Prianto GmbH
Barthstraße 18
80339 München

Tel.: +49 89 416148 290
services@prianto.com

Vertrauen ist gut, Sicherheit ist besser!

Einerseits gehen Gefahren von unvorsichtigen Nutzern aus (z.B. durch leichtfertigen Umgang mit Passwörtern) - andererseits von böswilligen Angreifern, deren Absichten Diebstahl, Manipulation oder Sabotage sind.
Ein schlüssiges Konzept zur Vermeidung und Abwehr von Insider-Angriffen (Insider Threat Mitigation) ist elementarer Bestandteil eines jeden, wirkungsvollen Cyber Security Plans.

Deshalb sind geeignete Schutzmaßnahmen in verschiedenen IT-Compliance Regelwerken verankert (TISAX, BAIT, PCI DSS, ISO27001, IEC 62443, DSGVO, ...) - und werden im Rahmen von Audits auch geprüft.
Die Nichtbeachtung oder nur teilweise Erfüllung, kann empfindliche Strafen und indirekte Schäden wie Imageverlust, Wettbewerbsnachteile, Abwanderung von Kunden etc. nach sich ziehen.

Viele Studien belegen einhellig, dass dringender Handlungsbedarf besteht. So schätzen sich 70-90% aller Organisationen selbst als anfällig für Insider-Angriffe ein. Wobei die Hälfte derartige Vorfälle schon zu verzeichnen hatten. Als Risikogruppen gelten gleichermaßen privilegierte Systembenutzer (Administratoren) und normale Anwender – sowohl Angestellte als auch Dienstleister.
Die beliebtesten Angriffsziele sind Datenbanken, Dateiablagen und Cloud Applikationen.

Ein „Insider Threat Mitigation Program "
kann in fünf Phasen und die dazugehörigen Maßnahmen gegliedert werden:

IDENTIFY - Sensible Systeme und Daten inkl. Zugriffsberechtigungen ermitteln
PROTECT - Angriffsfläche reduzieren
DETECT - Angriffe möglichst früh erkennen
RESPOND - Angriffe aufhalten, Angriffsmuster analysieren und ggf. Schwachstellen beseitigen
RECOVER - Rückkehr zum Normalbetrieb

Die Maßnahmen haben meist drei Dimensionen - Prozesse, Menschen und Technologie.
In größeren Unternehmen und Organisationen ist es nicht möglich die grundlegenden Prozesse manuell abzubilden.
Nur über geeignete Technologie und die damit erreichbare Automatisierung
kann die verlangte Qualität sichergestellt werden.
In jedem Falle spielt auch der Faktor „Mensch" eine entscheidende Rolle.
Nur wenn das Bewusstsein für die Notwendigkeit und den Sinn der Vorkehrungen geschärft ist,
wenden die Benutzer die bereitgestellten Mittel vorbehaltlos und wirkungsvoll an.

Prianto liefert geeignete, technische Hilfsmittel. Diese alleine bringen aber keinen Kunden zum Ziel.
Denn IT-Sicherheit ist nicht über das bloße Einschalten einiger Geräte erreichbar.
Unsere Partner steuern den viel wichtigeren Teil bei!
Sie kümmern sich um das Design und die Implementierung der Prozesse,
sowie um die Sensibilisierung und Schulung der Benutzer.
So entsteht am Ende ein Gesamtsystem, welches den gewünschten Zweck erfüllt.

Wir konzentrieren uns auf Produkte mit denen sich folgende „Best Practices" umsetzen lassen:

Benutzeridentitäten konsolidieren
Starke Authentifizierung einführen
Interne Verbreitungsmöglichkeiten auf andere Systeme („Lateral Movement") beschränken
Das „Least-Privilege-Prinzip" wahren
Logging und Monitoring aller über privilegierte Benutzerkonten ausgeführten Aktivitäten

Prianto Services GmbH
Barthstr. 18
80339 München

Tel.: +49 89 416 148 290
services@prianto.com

Geschäftsführer:
William Geens,
Lisa-Marie Moretti

USt-IdNr.: DE318578430
Finanzamt:
München für Körperschaften

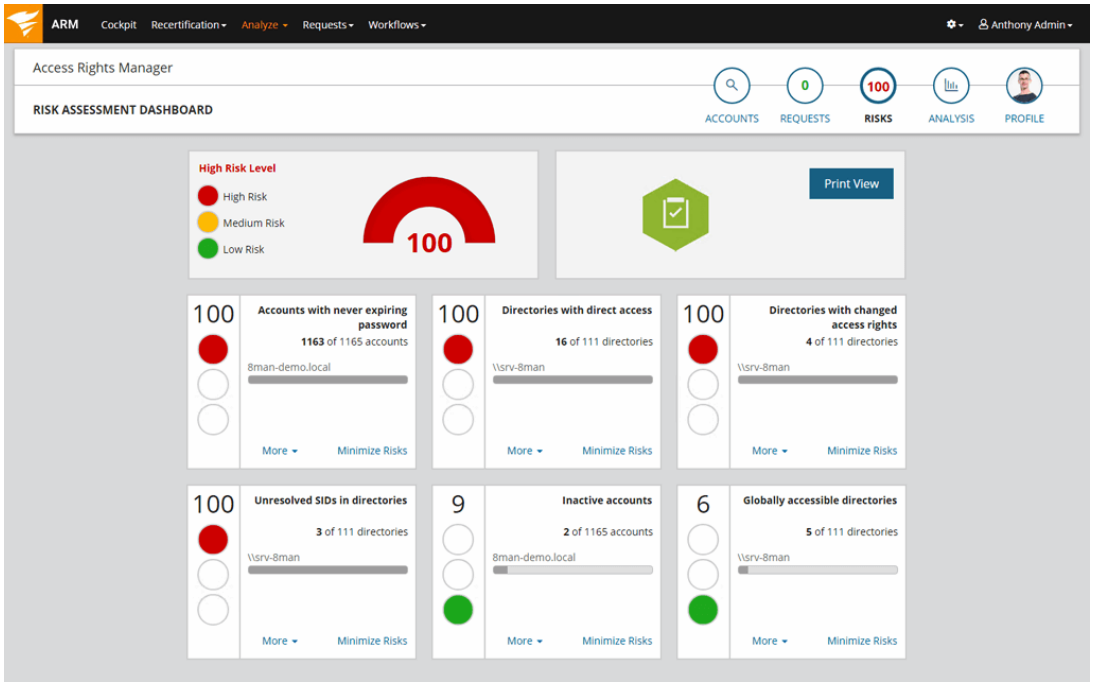
Deutsche Bank Soest
Swift-Code: DEUTDEDB416
IBAN: DE45416700240662301100

Registergericht München:
HRB240964

Access Rights Management – SolarWinds ARM

Über die Zeit gewachsene und immer dynamischer werdende Berechtigungsstrukturen für Active Directory, Windows-Dateifreigaben, SharePoint und Exchange zu beherrschen ist eine komplexe Herausforderung.
Bedingt durch fehlende Übersicht und Wildwuchs können sich erhebliche Sicherheitslücken auftun.
Oft erweisen sich die nativen Windows Bordmittel als unzureichend um dem wirkungsvoll zu begegnen.

Mit Solarwinds ARM kann man das Sicherheitsniveau und den Schutz vor internen Bedrohungen entscheidend erhöhen. Und zwar durch die Automatisierung der Verwaltung von Benutzerberechtigungen sowie die Analyse und die Durchsetzung von Richtlinien, wobei unsichere Benutzerkonten identifiziert und Audit-Trails erstellt werden. Die schnelle Erstellung von umfassenden Berichten zum Nutzerzugriff und zur Prüfung von Compliance schafft die nötige Transparenz. Benutzerberechtigungen und Authentifizierungen können mit automatisierter und vorlagenbasierter Bereitstellung und Aufhebung der Bereitstellung unkompliziert verwaltet werden.
Ein Self-Service-Portal lässt sich einsetzen, um die Zugriffsrechteverwaltung an die Dateneigentümer zu delegieren, was sich positiv auf die Produktivität auswirkt.



Mit Solarwinds ARM punkten unsere Partner bei ihren Kunden, dafür sprechen unzählige Referenzen.

Weiterführende Informationen:
Produktinformation: https://www.solarwinds.com/de/access-rights-manager
Technologie: https://support.solarwinds.com/SuccessCenter/s/access-rights-manager-arm
Anwendungsfälle: https://www.solarwinds.com/access-rights-manager#customerreviews
Demo Video: https://www.solarwinds.com/resources/video/solarwinds-access-rights-manager-overview
Downloadbereich Solarwinds - https://apps.prianto.pro/nextcloud/s/eoqAmCx7goQ8f7z

Prianto Services GmbH
Barthstr. 18
80339 München

Tel.: +49 89 416 148 290
services@prianto.com

Geschäftsführer:
William Geens,
Lisa-Marie Moretti

USt-IdNr.: DE318578430
Finanzamt:
München für Körperschaften

Deutsche Bank Soest
Swift-Code: DEUTDEDB416
IBAN: DE45416700240662301100

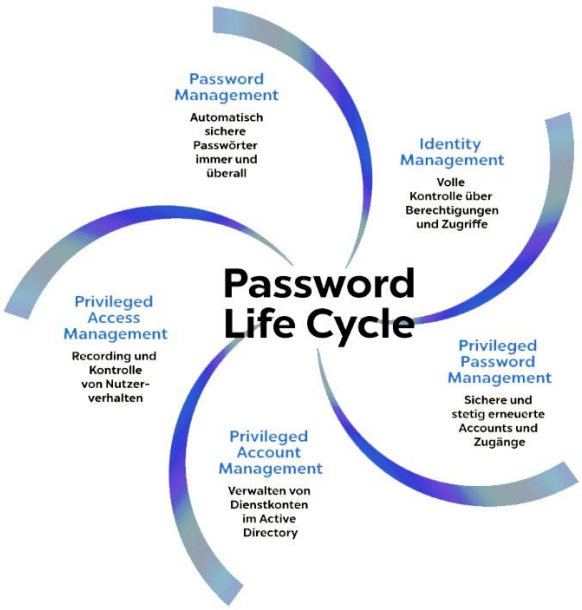
Registergericht München:
HRB240964

Enterprise Password Management – Mateso Password Safe

Die Anforderungen an Passwörter werden immer höher, aber komplexe Passwörter kann sich kaum jemand merken. Das führt oft zu Zettelwirtschaft und letztlich zu Sicherheitslücken im Unternehmen.
Oft nutzen mehrere Mitarbeiter einen Account gemeinsam, sodass nicht transparent ist, wer wann was in der entsprechenden Anwendung durchführt. Darüber hinaus finden sich häufig alte Accounts (z.B. Dienstkonten im Active Directory), deren Passwörter seit Jahren nicht geändert wurden und so unautorisierten Zugriff - z.B. von ehemaligen Mitarbeitern - ermöglichen. In den meisten Unternehmen gibt es keine geregelten Möglichkeiten im Notfall (Unfall, Krankheit) auf die Konten betroffener Mitarbeiter zugreifen zu können.

Password Safe dient als zentraler, digitaler Tresor zur Sicherung, Verwaltung und Überwachung von sensiblen Daten wie Passwörtern, (privilegierten) Zugängen und Konten. Berechtigungen können rollenbasiert bis auf Datensatz-Ebene vergeben werden. Die abgelegten Passwörter können für automatische Anmeldungen genutzt werden, ohne dass der Anwender diese einsehen kann. Durch den reichen Funktionsumfang eignet sich Password Safe für viele Szenarien, z.B. innerhalb der eigenen IT-Abteilung, für IT-Dienstleister oder im Bankenumfeld.

Funktionsumfang im Überblick:



Password Safe ist auch für sehr große Unternehmen geeignet - hoch skalierbar und fähig sehr komplexe Strukturen abzubilden. Als in Deutschland entwickeltes Produkt genießt es das besondere Vertrauen von über 10.000 Firmenkunden, darunter 20 der TOP 30 Dax-Unternehmen.

Weiterführende Informationen:

Video Tutorials: https://www.youtube.com/user/matesogmbh
Dokumente: https://www.prianto.com/hersteller-produkte/distribution/password-safe-by-mateso
Links: https://www.passwordsafe.de/features/produkt-tour/

Prianto Services GmbH
Barthstr. 18
80339 München

Tel.: +49 89 416 148 290
services@prianto.com

Geschäftsführer:
William Geens,
Lisa-Marie Moretti

USt-IdNr.: DE318578430
Finanzamt:
München für Körperschaften

Deutsche Bank Soest
Swift-Code: DEUTDEDB416
IBAN: DE45416700240662301100

Registergericht München:
HRB240964

Privileged Access Management – Hitachi HiPAM

Von privilegierten Benutzerkonten gehen erhebliche Gefahren aus. Das gilt sowohl für die klassische Informationstechnologie als auch für zunehmend vernetzte Systeme im Bereich der Produktion (Operational Technology). Fahrlässigkeit beim Umgang mit Zugangsdaten oder der Missbrauch von erweiterten Berechtigungen können weitreichende Schäden nach sich ziehen. Dazu gehören Datendiebstahl oder Systemausfälle und daraus resultierende Umsatzeinbußen, Strafen oder Reputationsverlust. Manuelle Prozesse für das Management von Benutzerkonten, Passworten und Berechtigungen sind aufwändig und fehleranfällig. Bei gemeinsamer Nutzung von Administratorkonten ist die Zurechenbarkeit von Aktionen nicht gegeben. Ist im Ernstfall ist mangels geeigneter Aufzeichnungen oft nicht nachvollziehbar was genau geschah, wodurch sich Fehlerbeseitigung und/oder Beweisführung schwierig gestalten. Die Beseitigung eben dieser Schwachstellen ist auch Gegenstand verschiedener Compliance Richtlinien bzw. der darauf basierenden Audits (ISO2700x, TISAX, BAIT, IEC62443 …)

Mit dem Hitachi Privileged Access Manager [HiPAM] kann man den mit privilegierten Benutzerkonten verbundenen Risiken wirkungsvoll begegnen. Für jede Anforderung in den Bereichen Sicherheit, Nachweisbarkeit und Konformität gibt es passende Module bzw. Funktionen. Um den Aufwand für Design und Implementierung möglichst gering zu halten, sind vorgefertigte Regelwerke und Prozesse verfügbar [Hitachi ID Identity Express - Privileged Access Edition]. HiPAM ist ein wichtiger Baustein für ihr ISMS. Alle Anforderungen der ISO 27001 bzgl. Privileged Access Management, wie z.B. Annex 9.2.3 – lassen sich damit schnell, einfach und günstig erfüllen!

HiPAM ermöglicht für die angebundenen Systeme und Konten das Erstellen von Rollenmodellen und Zugriffsregeln, welche festlegen wer sich wo mit welchen Konten anmelden kann. Vorhandene Benutzerverzeichnisse können angebunden werden. Anmeldevorgänge werden zwischen Systemen und Benutzern vermittelt (Starke Authentifizierung und Single Sign On) und Sitzungen aufgezeichnet (Session Recording). Per Auto-Discovery können neue Systeme angebunden und regelbasiert klassifiziert werden. Genehmigungsprozesse sind automatisierbar und können auch mit Ticket Management Systemen gekoppelt werden um Aktionen in freigegebene Wartungsfenster zu lenken. Zufallsgenerator und Rotation für Passworte können zeitgesteuert laufen. Ein übersichtliches Dashboard und Möglichkeiten für Analysen sind gegeben. Ebenso die Möglichkeit über Smartphone Apps per SSH und RDP zu arbeiten.

Ein wesentliches Merkmal der Architektur sind die zahlreichen Konnektoren, sodass das System ohne Sprungserver auskommt. Auch deshalb eignet sich HiPAM besonders gut für Managed Service Provider, um sehr wirtschaftlich ein zentralisiertes, mandantenfähiges System aufzubauen. Dazu passende Lizenzierungsoptionen sind geboten.

Hitachi PAM ist sehr wettbewerbsfähig bepreist - dem Partner ist es möglich eine attraktive Marge durchzusetzen.

Weiterführende Informationen:
Produktinformation: https://hitachi-id.com/documents/#brochure
Whitepapers: https://hitachi-id.com/documents/#brochure,%20.white-paper
Case Studies: https://hitachi-id.com/aboutus/casestudies/casestudies.html
Webinar: https://hitachi-id.com/documents/#webinar

Prianto Services GmbH
Barthstr. 18
80339 München

Tel.: +49 89 416 148 290
services@prianto.com

Geschäftsführer:
William Geens,
Lisa-Marie Moretti

USt-IdNr.: DE318578430
Finanzamt:
München für Körperschaften

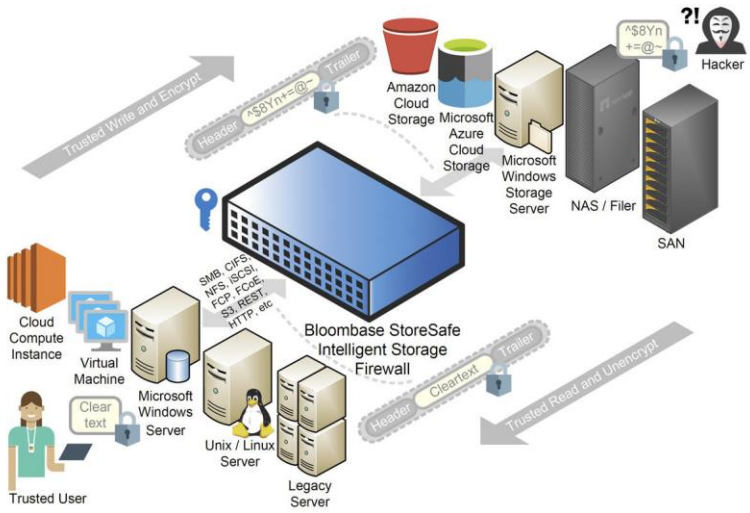
Deutsche Bank Soest
Swift-Code: DEUTDEDB416
IBAN: DE45416700240662301100

Registergericht München:
HRB240964

File & Folder Encryption – BLOOMBASE StoreSafe

Vertrauliche und geheime Informationen in Dateiablagen sind ein beliebtes Angriffsziel.
Gelangen intellektuelles Eigentum, Verträge, Patientendaten, Kreditkartendaten o.ä. in die falschen Hände, kann sehr großer Schaden entstehen. BLOOMBASE StoreSafe eignet sich hervorragend um Dateien und Ordner so zu verschlüsseln, dass nur autorisierte Personen Zugriff haben.
Rollenmodelle ermöglichen die granulare Verteilung von Rechten. Informationseigentümer (Data Owner) können die zugriffsberechtigte Benutzergruppe (Data Operator) selbst bestimmen.
Systemadministratoren (Service Operator) können ihre Arbeit ungehindert verrichten, obwohl sie keinen Einblick haben.
Die Ver- und Entschlüsselung findet – für den Client transparent - im StoreSafe statt, einem im Netzwerkpfad zwischen Client und Storage (NAS, File Server) befindlichen Encryption-Proxy.
Die Netzwerkverbindung zwischen Client und StoreSafe kann mit IPSec gesichert werden.
Die Authentifizierung ist über das Active Directory möglich, ggf. kombiniert mit einer Zwei-Faktor-Authentisierung.
Das System ist Software Defined, d.h. für den Betrieb auf Standard Servern konzipiert.
Entweder als Virtual Appliance auf einem „Virtualization Host" oder direkt auf Windows bzw. LINUX als Betriebssystem. Bei Bedarf kann das System als active-standby Cluster ausfallsicher ausgelegt werden.
Auf den Clients muss keine Software installiert werden, was die Implementierung und den Betrieb erheblich vereinfacht. Für die sichere Verwaltung und Verwahrung der Schlüssel kann das komplementäre Produkt KeyCastle oder auch ein anderes, KMIP-kompatibles System eingesetzt werden.

Die Dimensionierung des Systems erfolgt durch Zuweisung einer angemessenen Zahl von Prozessorkernen, welche auch die (faire) Basis für die Lizenzierung darstellt.



Weiterführende Informationen:
Produktinformation: https://www.bloombase.com/products/spitfire/storesafe/resources.html
Technologie: https://www.bloombase.com/technology/index.html
Anwendungsfälle: https://www.bloombase.com/solutions/index.html
Downloadbereich Bloombase - https://apps.prianto.pro/nextcloud/s/AcpfKrXn8RsGrHd

Prianto Services GmbH
Barthstr. 18
80339 München

Tel.: +49 89 416 148 290
services@prianto.com

Geschäftsführer:
William Geens,
Lisa-Marie Moretti

USt-IdNr.: DE318578430
Finanzamt:
München für Körperschaften

Deutsche Bank Soest
Swift-Code: DEUTDEDB416
IBAN: DE45416700240662301100

Registergericht München:
HRB240964