

ProCloud

Security Produkt

Portfolio

Sehr geehrte Damen und Herren

Das Nationale Zentrum für Cyber-Sicherheit (NCSC) des Bundes meldete im Verlaufe des 2020 einen Anstieg von bis zu 300% an Cyber-Vorfällen. Neben Grossunternehmen sind auch KMUs besonders stark betroffen.

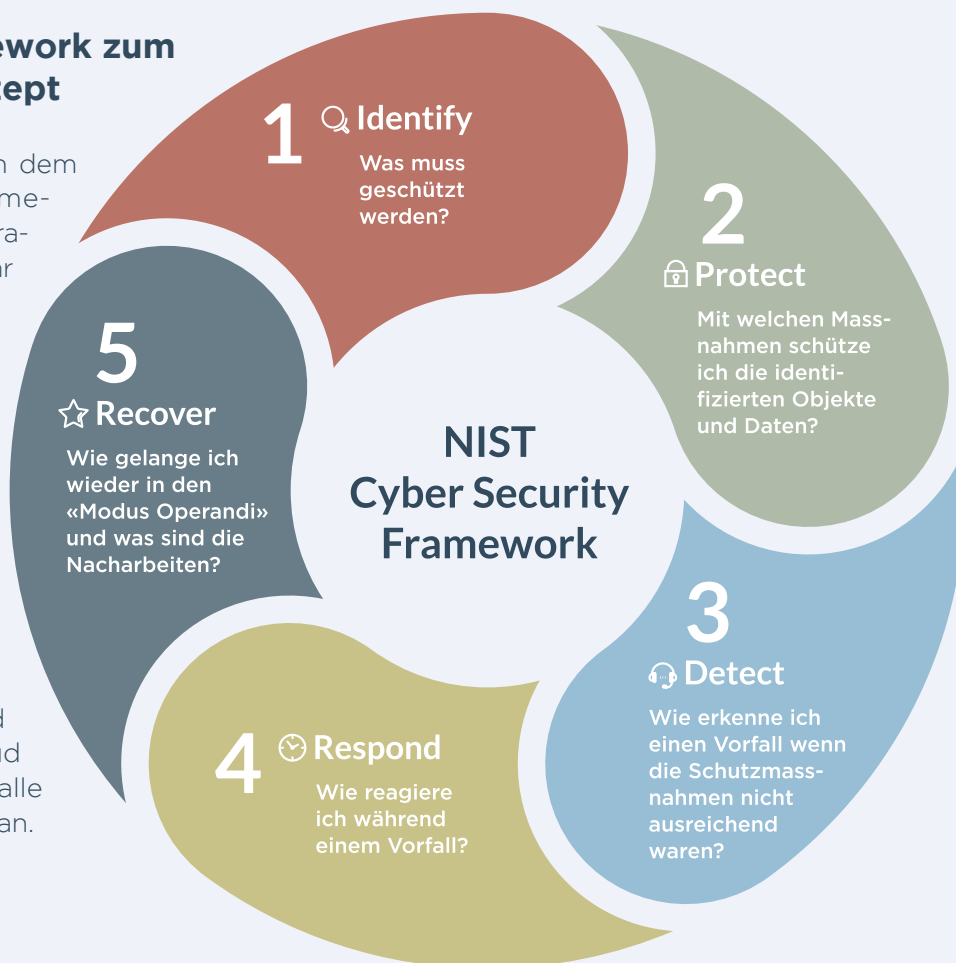
Während im Jahr 2010 noch Antivirus, Firewall und Backup ausreichend waren, haben sich die Angreifer in den letzten Jahren professionalisiert. Ransomware, Angriffe mit Unterstützung künstlicher Intelligenz und personalisierte Angriffe passieren 24/7.

Es ist in Ihrer Verantwortung als Unternehmen, sich über das derzeit grösste Unternehmensrisiko zu informieren und sich zu schützen.

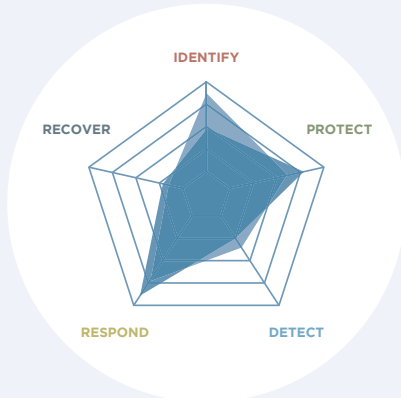
Die ProCloud AG unterstützt Sie strukturiert im Kampf gegen die Cyber-Risiken.

Mit dem NIST-Framework zum Cyber Security Konzept

Die ProCloud arbeitet nach dem NIST-Cyber-Security-Framework. Das Cyber-Security-Framework wurde bereits im Jahr 2014 von NIST – dem National Institute of Standards and Technology – veröffentlicht. Aufgrund seiner einfachen Verständlichkeit, kombiniert mit der hohen Substanz, verbreitete es sich rasch auch in der Privatwirtschaft. Auch die ProCloud AG setzt auf das NIST-Cyber-Security-Framework. Wir setzen es für eine 360° Grad Sicht und Beratung ein. Die ProCloud AG bietet ausserdem für alle Phasen des NIST Produkte an.



Unser Produkt Portfolio zum NIST Cyber Security Framework



Security Assessment

Alle, identify, respond, recover

Bereits enthalten in: 1h kostenloses NIST Review für Desktop as a Service Kunden

Wir legen grossen Wert darauf, dass Ihre IT Security auch für Sie ein greifbares und praktikables Thema ist. Basierend auf unserer Analyse der Ausgangslage, erarbeiten wir mögliche, umsetzbare Verbesserungen für Ihr Unternehmen.

- ✓ Gemeinsame Definition des Umfangs
- ✓ 360-Grad-Übersicht über die Ausgangslage
- ✓ Report mit Empfehlungen zu Massnahmen



Enterprise Cyber Defense Center

detect, respond

Unser Enterprise Cyber-Defense-Center verbindet die Stärken der weltweit führenden künstlichen Cyber-Intelligenz mit unserem schnellen und effizienten 24/7 Security-Operation-Center.

- ✓ Selbstlernendes Enterprise Immune System
- ✓ Proaktives Security-Operation-Center (24/7)
- ✓ Vollständige Abdeckung der gesamten IT (on-premise, Cloud, M365, usw.)
- ✓ In weniger als einer Stunde installiert

Das Enterprise Immune System ist eine Echtzeit-Bedrohungserkennung auf dem Netzwerk-Layer. Es kombiniert das Know-how der besten menschlichen Cyber-Analysten mit der Geschwindigkeit von künstlicher Intelligenz und Machine Learning.



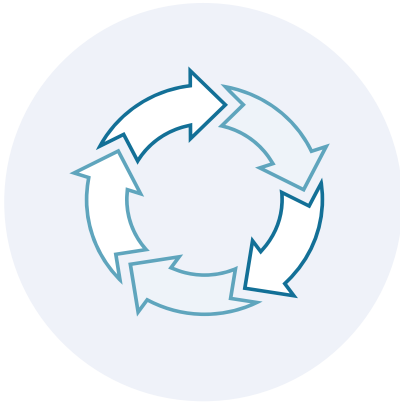
User Security + Support Flat Fee

identify, protect

Unsere User Support Flat Fee ermöglicht Support zum Fixpreis. Mit dem Upgrade «Security» erhalten Sie aber noch viel mehr als das:

- ✓ User Support Flat Fee (drei Geräte/Person)
- ✓ Awareness Training durch regelmässige Phishing Simulationen
- ✓ Device Management (Inventarisierung, Windows Update Management, Antivirus)

Unser Produkt Portfolio zum NIST Cyber Security Framework



Managed Asset

identify, protect

Bereits enthalten in: ProCloud Desktop as a Service

Mit unseren Managed Services kümmern wir uns von der Inventarisierung bis hin zum vollständigen und proaktiven Management (Überwachung, Update- & Incident-Management, usw.) um Ihre Assets. Zum Beispiel:

- ✓ Managed Server
- ✓ Managed Azure / AWS / GCP Services
- ✓ Managed Firewalls
- ✓ Managed Devices

Mehr Infos unter: [procloud.ch/managed](https://www.procloud.ch/managed)



Cloud Backup

protect, recover

Bereits enthalten in: ProCloud Desktop as a Service

Die Fähigkeit unserer Cloud Backup Lösungen ist «alles nach überall» sichern zu können. Es gibt fast nichts, das wir nicht sichern können und wir können es in unsere Datacenter, wie auch an beliebige Ziele tun (zbsp. Microsoft Cloud, Kunden Standort etc.). Wir führen dazu drei Produkte:

- ✓ Enterprise Cloud Backup
(inkl. vollständiges Management und kostenlosen Recovery Tests)
- ✓ KMU Cloud Backup
(selbständiges Management durch den Kunden)
- ✓ Veeam Cloud Connect

Das Cloud Backup hilft in erster Linie die RPO⁽¹⁾ Dauer zu reduzieren und ermöglicht lange Aufbewahrungszeiten.

⁽¹⁾ **Recovery Point Objective (RPO)**

Wie viel Datenverlust kann in Kauf genommen werden? (Zeitangabe)

Unser Produkt Portfolio zum NIST Cyber Security Framework

New!



Automated Security Awareness Platform

identify, protect

Mehr als 80 % aller Cyber-Sicherheitsvorfälle entstehen durch menschliche Fehler und die Folgen sind fatal. Oftmals gelingt es nicht, den Mitarbeitenden die gewünschte Verhaltensweise und die erforderliche Motivation in Bezug auf die Cyber-Sicherheit zu vermitteln.

Mit unserem Produkt «Automated Security Awareness Platform» bieten wir Ihnen die passende Lösung:

- ✓ Online-Tool zur Förderung der Cyber-Sicherheit Kenntnisse der Mitarbeitenden
- ✓ Schnelle und unkomplizierte Einführung
- ✓ Abwechslungsreiche Module, damit die Mitarbeitenden am Ball bleiben: E-Mail, Surfen im Internet, Passwörter, Soziale Netzwerke und Messenger, PC-Sicherheit, mobile Geräte, Vertrauliche Daten, Persönliche Daten/DSGVO, Social Engineering, Sicherheit zu Hause und unterwegs

Die Plattform verspricht 90 % weniger Vorfälle und 93 % Wahrscheinlichkeit, dass das Wissen bei der täglichen Arbeit angewendet wird. Dabei sind 86 % der Teilnehmer bereit, das Programm weiterzuempfehlen.

New!



Phishing-Simulation

identify, protect

Um sich ersten Zugang zu Systemen zu verschaffen, nutzen 65 % der Angreifergruppen Phishing-Attacken. Dabei wird 94 % der Malware per E-Mail zugestellt. Dieses Risiko kann mit Awareness-Trainings für die Mitarbeitenden nachweislich gesenkt werden. Unsere regelmässige Phishing-Kampagne (vierteljährliche Zyklen, einmalig oder gestaffelt) können genau hier Abhilfe verschaffen.

Wir übernehmen die Rolle der Angreifergruppe und stellen Ihnen echt aussehende E-Mails zu, mit dem Ziel, dass die Benutzer*innen interagieren.

- ✓ Auswertung in Form eines Managementberichtes mit Details zu Ansichten und Aktionen pro Benutzer*in
- ✓ Steigerung der Awareness bei allen Mitarbeitenden
- ✓ Einfacher und effektiver Schutz im Bereich Prävention

Unser Produkt Portfolio zum NIST Cyber Security Framework

New!



ProVault

protect, recover

Unser ProVault Speicher ist eine Disaster Recovery Versicherung. Es ist eine Detail-konzipierte Lösung, um das Risiko eines Totalverlustes auf ein Minimum zu reduzieren und beinhaltet:

- ✓ Vollständig unabhängiges Datacenter (ISO 27001, Tier-3 Level)
- ✓ Vollständig getrenntes Management des Datacenters ohne gemeinsame Nenner
- ✓ Mehrere unabhängige Sicherheitszonen
- ✓ Offline Storage (sogenannter «Air Gap»)

Aktuell bieten wir dieses Produkt als Veeam Cloud Connect VM Backup Service und zusätzlich für Produkte an, die bei uns im Datacenter betrieben werden (Desktop as a Service, Infrastructure as a Service).



Instant Recovery

protect, recover

Bereits enthalten in: ProCloud Desktop as a Service

Unser Instant Recovery Produkt ist ausschliesslich für unsere Datacenter Kunden verfügbar. Es befindet sich physisch getrennt von der primären Infrastruktur, in einer separierten Zone. Instant Recovery dient einem maximalen RTO⁽¹⁾ Erlebnis im Disaster Fall.

⁽¹⁾ **Recovery Time Objective (RTO)**
Wie lange darf ein Geschäftsprozess/System ausfallen? (Zeitangabe)

- ✓ Physisch getrennte Zone (eigener Brandabschnitt)
- ✓ Backup auf vollständig SSD basierten High Performance Storage
- ✓ Instant Recovery der virtuellen Server auf dem Backup Storage möglich (der Recovery Vorgang läuft währenddessen im Hintergrund und muss nicht abgewartet werden)

Weitere Schritte

Wir sind ein Cloud-Services und Cyber-Security fokussiert Dienstleister. Bei Fragen stehen wir Ihnen also gerne zur Verfügung. Kontaktieren Sie direkt Ihren persönlichen Betreuer oder melden Sie sich unter +41 62 552 01 00 / info@procloud.ch. Wir freuen uns auf Sie!

**Autor**

Patrice Steiner
Cloud Security Engineer /
IT-Sicherheitsverantwortlicher
info@procloud.ch
+41 62 552 01 00

Sie brauchen keine IT

Sie brauchen einen Service

ProCloud AG
Sägestrasse 50
5600 Lenzburg

+41 62 552 01 00
info@procloud.ch
www.procloud.ch