PKA LOG-SERVER

SICHERN SIE IHRE LOG-DATEN NACH DEN AKTUELLEN DATENSCHUTZ-GESETZEN

- **PKA speichert alle Ihre dezentralen Log-Dateien auf einen Server bzw. Server-Farm**
- **In größeren Umgebungen werden die Log-Server pro Standort kaskadiert aufgebaut**
- **Die Speicherung, Analyse, Auswertung und Abfrage erfolgen nach den aktuellen Datenschutz-Richtlinien**

Sowohl der Gesetzgeber als auch das Bundesamt für Sicherheit in der IT legen die zentrale Protokollierung nahe, ohne diese explizit zu fordern. Gefordert wird nur die Auswertbarkeit.
In einer verteilten heterogenen Umgebung können Sie aber nur zentral auswerten.
Der PKA Service speichert alle Ihre Log-Dateien zentral.

GRUNDLAGEN DER PROTOKOLLIERUNG:

Nachweisbarkeit:

Der Gesetzgeber fordert unter anderem im Gesetz zur Kontrolle und Transparenz (KonTrG) die Nachweisbarkeit, wer welche Daten wann verändert hat.

Unveränderbarkeit:

Die Log-Dateien werden nur verschlüsselt übertragen und gespeichert.
Die Verschlüsselung der Kommunikation und der Daten schützt vor Veränderungen.

INFORMATIONSFLUSS:

Der Client sendet Ihre Log-Daten an Ihren jeweiligen Log-Server. Sollte der Log-Server temporär nicht erreichbar sein, versucht der Client die Speicherung mehrmals in wechselnden Zeitfenstern zu wiederholen. Der Client sendet nach dem dritten Fehlversuch eine Warnung an den Administrator und versucht die Daten an den zentralen Server zu senden. Das Versenden wird ebenfalls protokolliert und kann später ausgewertet werden.

Die Daten auf den Clients werden anschließend gelöscht und von neuen Einträgen überschrieben. Der Log-Server wird von PKA als Service zur Verfügung gestellt damit PKA Ihre Protokollierung durchführen kann. Sie erwerben keinen eigenen Server.

Mögliche Log-Clients sind:

- alle Microsoft Systeme aller Versionen
- Linux
- Unix
- Firewall
- IDS/IPS (Intrusion and detection / prevention)
- Proxy-Server
- Web-Server
- Datenbanken
- Applikations-Server

Der Zugriff auf die Log-Dateien

Der Zugriff auf die Log-Dateien und deren Auswertung erfolgt nach strengen Richtlinien und wird ebenfalls protokolliert. Die Auswertung erfolgt zweckgebunden. Nachweis einer Straftat.

- Fehlersuche
- Fehlervorhersage
- Einbruchsanalyse
- Mitarbeiterverhalten kann nicht ausgewertet werden.

Löschen der Einträge

Das Löschen ist Pflicht und wird nach den lokalen Gegebenheiten, Gesetzgebung und internen Regelung angepasst, durchgeführt und protokolliert.

Optional

Die Auswertungen werden in übersichtlichen Tabellen dargestellt.
Eine graphischen Darstellung, auch mobil, ist optional.
PKA hilft Ihnen gerne bei der Auswertung und deren Bewertung.

DER PKA LOG-SERVER SPEICHERT DIE LOG-EINTRÄGE NACH 3 PRINZIPIEN:

1 **Auswertung Basismodus**

In der Basis Version speichert der Log-Server nur die vom Gesetzgeber geforderten Log-Einträge. Es erfolgt keine Auswertung. Die administrativen Tätigkeiten werden gespeichert und unterliegen einer besonderen Sicherheitsstufe, so dass kein Administrator diese löschen oder verändern kann.

2 **Auswertung Produktionssicherung & Fehlervorhersage**

In der zweiten Version werden mehr Einträge gespeichert. Alle Einträge, die zur Produktionssicherung dienen und dienen könnten, werden gespeichert.
Es werden automatisch und manuell Netzwerk und System Fehler in der Auswertung verarbeitet. Sobald ein Fehler erkannt wurde, sucht das System in den historischen Daten nach einem Muster der Wiederholbarkeit und nach dem Auslöser des Fehlers.
Durch dieses Verfahren kann eine Fehlervorhersage durchgeführt werden.
Sobald die Ursache eines Fehlers wiederauftritt und der Musterverlauf eintritt, wird der Administrator gewarnt.

3 **Auswertung nach dem PKA pre-crime Verfahren zur Einbruchsanalyse**

Die Log-Einträge können zur Einbruchsanalyse verarbeitet werden.
Dazu werden die NSA Empfehlung zur Protokollierung herangezogen.
Die Auswertung wird zusammen mit dem PKA pre-crime Verfahren zur Einbruchsvorhersage genutzt.

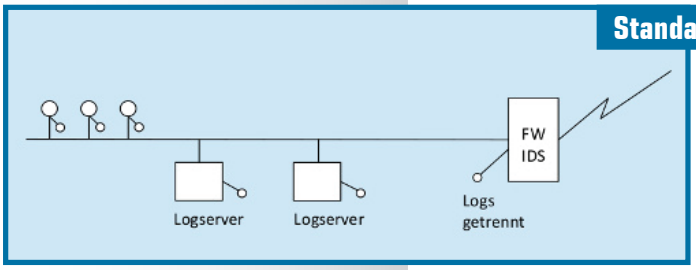
ZIELE:

1. Datenschutzrechtlich konforme Speicherung aller Logs.
2. Automatische Auswertung zur Produktionsabsicherung
3. Automatisches Erkennen von Hackerangriffen
4. Automatisches Erkennen von Virenaktivitäten
5. Erhöhung der IT Sicherheit
6. Automatische Abwehr gegen Cyberterror und Cyberangriffe durch die Integration mit dem PKA NFN

IHR VORTEIL:

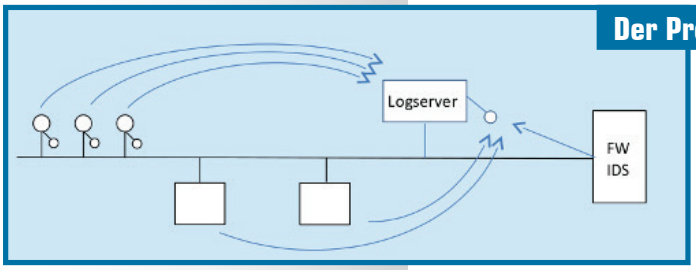
- Der Kunde braucht sich nicht mehr um seine Protokollierung zu kümmern.
- Die Protokollierung unterliegt den aktuellen Datenschutzrichtlinien.
- Die selektierten Auswertung sind automatisiert und vergleichen aktuelle Ereignisse mit den vergangenen und zukünftigen.
- Somit eignet sich die zentrale Log-Speicherung und Analyse für kleine, mittlere und große Unternehmen.

GRAFISCHE DARSTELLUNG:



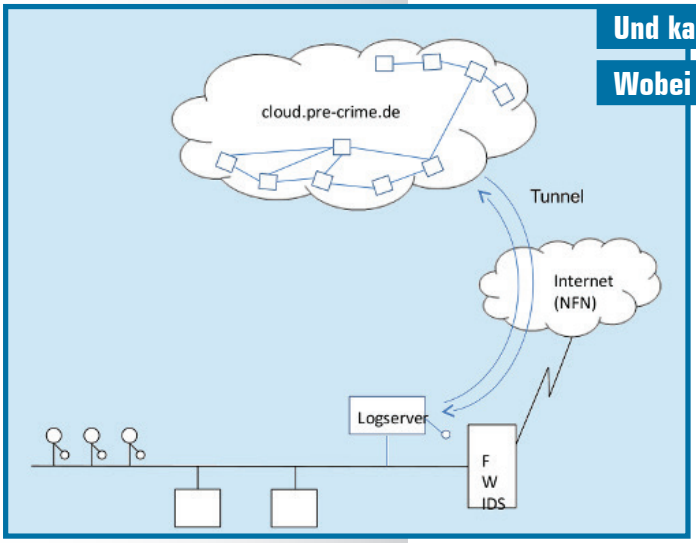
Standard Netzwerk, ohne PKA Log-Server Service.

Ihre Rechner im Netzwerk haben alle, wenn überhaupt, ein eigenes Log-File. Die Log-Daten entsprechen möglicherweise den Anforderungen des Bundesdatenschutzgesetzes. Eine Auswertung findet nicht statt.
Eine Angriffserkennung ist so nicht möglich.



Der Pre-Crime Log-Server erhält alle Log-Files aus Ihrem Netzwerk.

Die Protokollierung erfolgt nun nach den aktuellen Gesetzgebungen. Die Auswertung erfolgt zentral auf Ihrem Log-Server. Es können alle Log-Files verarbeitet werden. Das gilt auch für: Mail-Server, Update-Server, Antiviren-Server usw…



Und kann mit der Cloud zusammen arbeiten.

Wobei keine internen Daten versendet werden. Nur Angriffsmuster.

Ihr zentraler Log-Server kommuniziert mit dem zentralen Pre-Crime Server.
Die Pre-Crime Cloud bildet eine zentrale Intelligenz und führt die Internet-Auswertungen durch.

Pre-Crime

System zur vorhersagbaren Verteidigung von Hackern