Windows Angriffe abwehren mit LogApp

DI Alexander Graf
Stefan Synek
iQSol GmbH

Überblick

Vorstellung

Angriffe mittels Powershell

Vorgangsweise und Erkennung/Abhilfe (Live Demo)

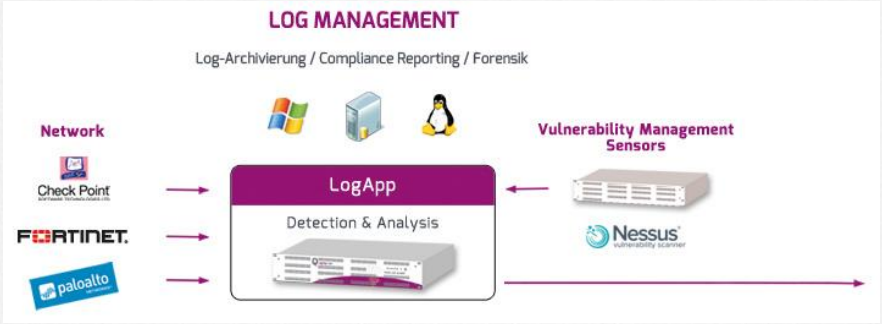
Vorstellung

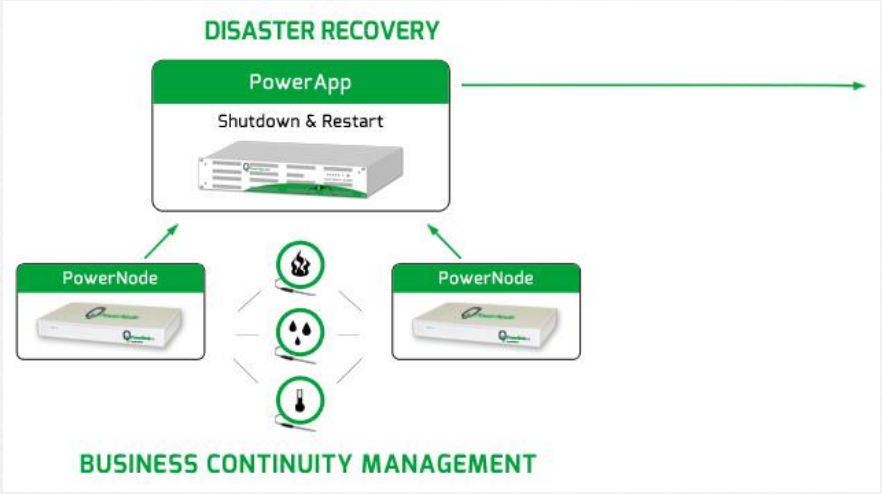
iQSol – IT-Security made in Austria

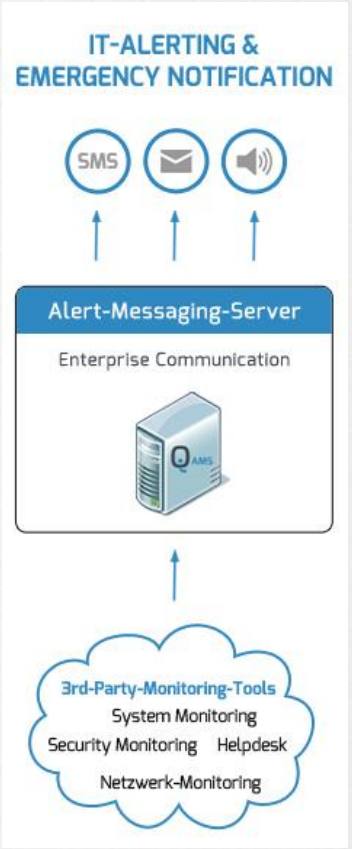
- **iQSol als Security Softwarehersteller** - ein Spin-Off der Antares NetlogiX („100% made in Austria“)

Sicherheit 360°

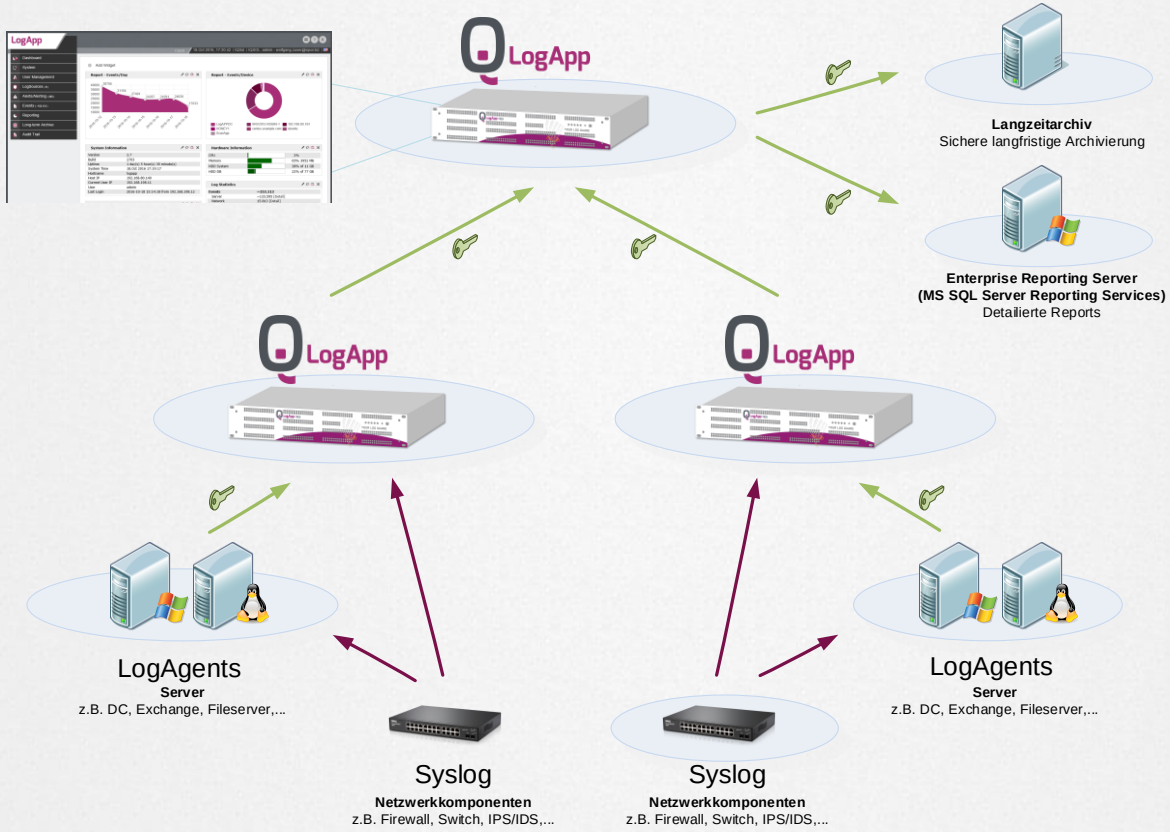
- **DSGVO konformes Log Management**
- **Integritäts Monitoring**
- **Alerting**
- **Disaster Recovery**
- **MSSP fähig**







LogApp Architektur

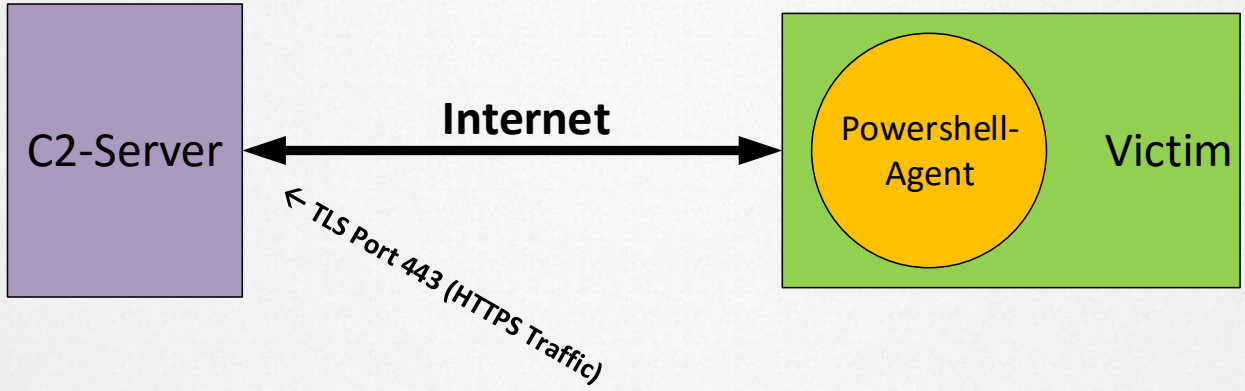


Angriffe mittels Powershell

Powershell ist

- ein wertvolles Werkzeug zur Windows-Administration
- unterstützt IT-Profis bei der Automatisierung von Aufgaben

Unglücklicherweise verwenden Cyberkriminelle zunehmend Powershell



Vorgangsweise und Erkennung/Abhilfe

<u>Angreifer:</u> Wie kann ich einem Opfer den PS-Agent unterjubeln?

Dokumente mit gefährlichem Inhalt (Word, Excel, PowerPoint, etc.)

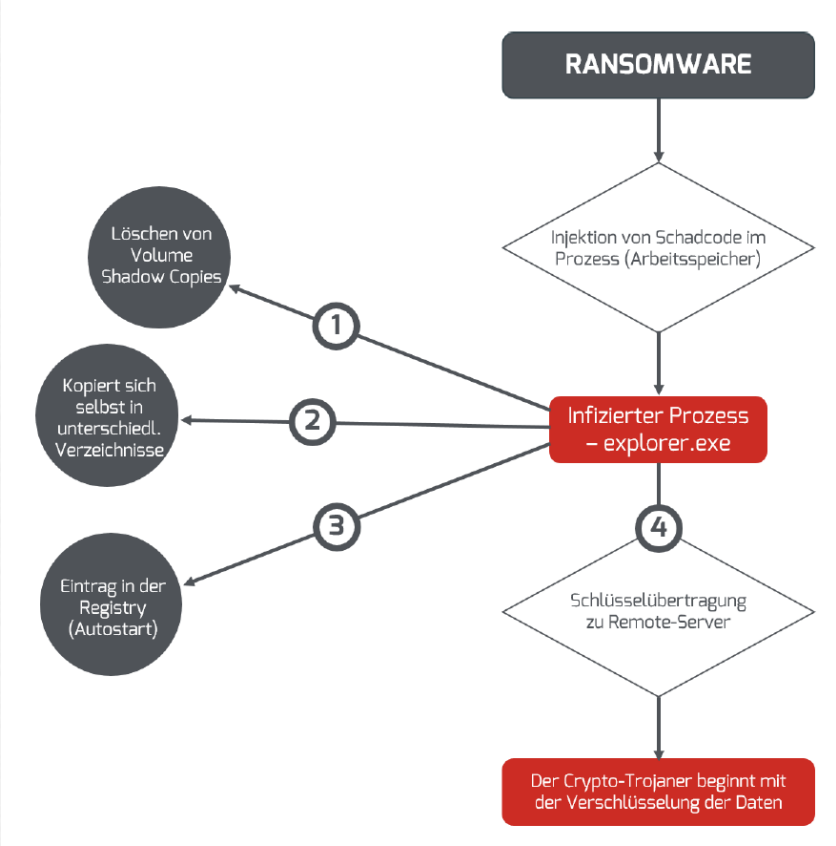
Verwendung spezieller Hardware („USB-Stick“)

<u>Opfer:</u> Wie kann ich erkennen, das ich Ziel eines Angriffs wurde?

- angemessenes ***Security Information und Event Management***

LogApp
Security Information & Event Management

Windows Enhanced Security



Windows Enhanced Security

1) Volume Shadow Copies

Die Ausführung eines Kommandos zur Manipulation von Volume Shadow Copies (vssadmin.exe) ist äußerst selten. Diese Aktivität sollte alarmiert und untersucht werden.

2) Ausführen von Daten in einem Ordner

Das Ausführen von Daten in einem Ordner wie bspw. C:\Windows\Temp oder C:\Users\<user>\AppData\ ist sehr verdächtig und sollte demnach unterbunden werden. Ein Alarm sollte diesbezüglich ebenfalls ausgelöst werden.

3) Einträge in die Autostart-Registry

Einträge in die Autostart-Registry sollten ebenfalls alarmiert und untersucht werden.

4) Prozesse, die mit dem Internet kommunizieren

Prozesse, die normalerweise nicht mit dem Internet kommunizieren können, sind höchst verdächtig. Falls so ein Prozess eine Verbindung aufbaut, sollte dies umgehend untersucht werden.

Vorgangsweise und Erkennung/Abhilfe

1) Ausführung des .bat Files am Victim Server

   ↳ LogApp erkennt **„[WES] Powershell Activity / Suspicious Powershell parameters detected“**

2) Shadow Copy erzeugen

   ↳ LogApp erkennt **„[WES] Shadow Copy Detection / Shadow copies were listed“**

3) Registry-Eintrag erzeugen

   ↳ LogApp erkennt **„[WES] Persistence / Registry value for Autostart modified“**

4) Kommunikation PS-Agent → C2 Server

   ↳ LogApp erkennt **„[WES] Powershell Activity / Powershell created network connection“**

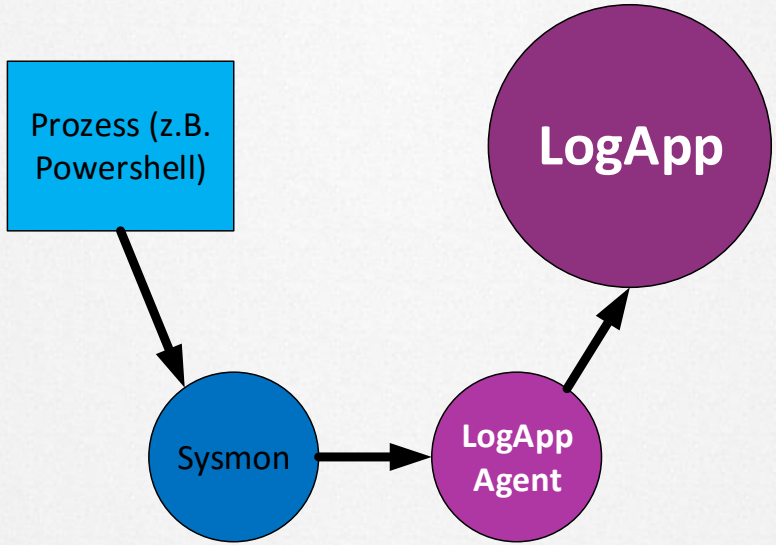
5) AD-User anlegen

   ↳ LogApp erkennt **„[WES] Account Usage / Windows: user added to privileged group“**

Vorgangsweise und Erkennung/Abhilfe

Wie funktioniert die Erkennung mittels LogApp grundsätzlich?

Workflow Sysmon Infos



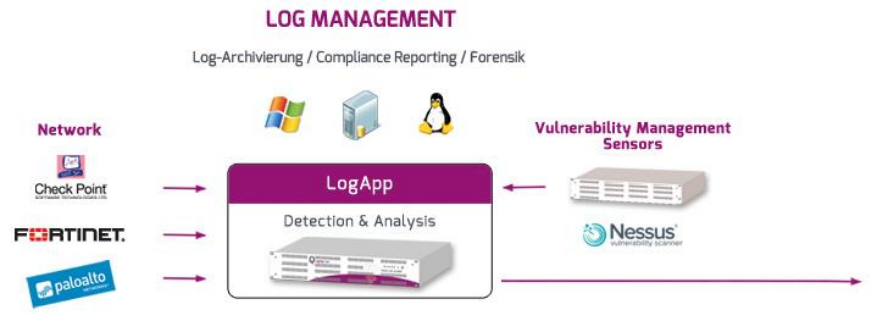
Live Demo LogApp

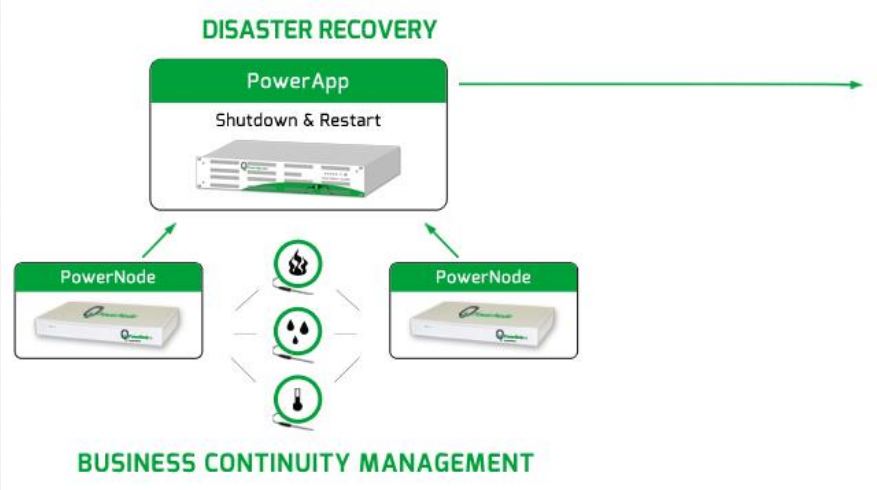
Vielen Dank für Ihre Aufmerksamkeit!

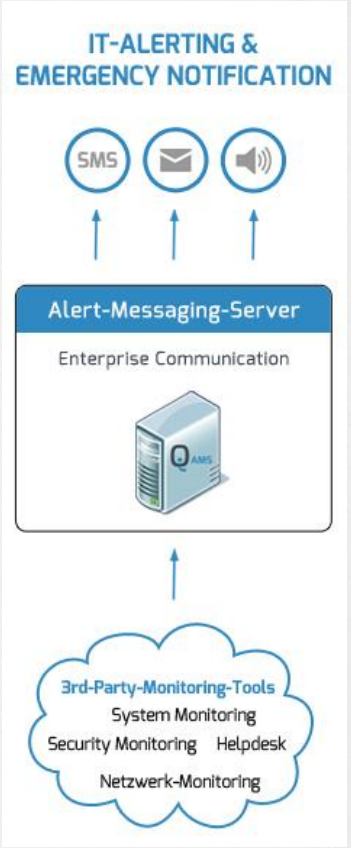
Kontakt:

www.iqsol.biz

alexander.graf@iqsol.biz







Thanks to our Sponsors!