klopfer datennetzwerk gmbh

arcserve

SOPHOS

klopfer.com

Backup-Security 2020 - so schützen Sie sich mit Arcserve und Sophos

1. **Ausblick Cyberbedrohungen 2020**

   Stefan Burkhardt, klopfer datennetzwerk gmbh

2. **arcserve & Sophos als Verteidigungslinie gegen Ransomware**

   Sven Haubold, Arcserve GmbH

3. ***Sophos EDR - Mit Forensik und Synchronized Security den Kampf gegen Emotet und Co. gewinnen***

   Björn Zackenfels, Sophos Technology GmbH

Herausforderungen

- zunehmende Digitalisierung und Vernetzung, das Internet der Dinge oder Smart Home bieten den Angreifern immer neue Angriffsflächen
- zunehmende Professionalisierung der Angriffe (Bulletproof-Hosting-Services, Ransomware-as-a-Service)
- täglich werden rund **400.000** neue Schadprogrammvarianten entdeckt
- die Anzahl von Spam-Nachrichten mit Schadsoftware im Anhang ist in jüngster Zeit um über 1.000 Prozent angestiegen
- klassische Abwehrmaßnahmen verlieren weiter an Wirksamkeit bzw. werden häufig nicht oder unzureichend umgesetzt
- im Fokus der Angriffe stehen Unternehmen und kritische Infrastrukturen, Verwaltungen, Forschungseinrichtungen aber auch Privatpersonen
- Bewertung Unternehmensrisiko „Cybervorfälle“ stieg in den letzten Jahren von Platz 15 auf Platz 2 (Allianz RiskBarometer)

klopfer
datennetzwerk gmbh

Was ist Emotet?

- Trojaner, der vor allem durch Spam-E-Mails verbreitet wird
- enthält bösartige Skripte, Dokumente mit aktivierten Makros oder bösartige Links
- sind oft gut gefälscht und täuschend echt als reguläre E-Mails getarnt
- ein polymorpher Virus = der Code wird bei jedem neuen Abruf leicht verändert
- erkennt virtuelle Maschinen und Sandbox-Umgebungen

Was macht Emotet so gefährlich?

- ergreift Besitz von Ihrer Kontaktliste und versendet sich selbst an Mitarbeiter und Kunden
- Absender dieser E-Mails wird jedoch stets Ihr richtiger Name angezeigt
- bei Zugriff im Netzwerk weitere Ausbreitung
- probiert Passwörter aus, um auf weitere Ressourcen zuzugreifen
- Spezielle Fähigkeiten und Eigenschaften
- greift sowohl Firmen als auch Endbenutzer an
- kann andere Schadsoftware nachladen und sich in Netzwerken verbreiten
- missbraucht Kontakt-Informationen aus Outlook
- späht die ersten 16kB jeder E-Mail aus (Textkopie einer Originalmail)

klopfer
datennetzwerk gmbh

Warum ist das so einfach?

- mittels Cloud-Technologie über das Internet angebotener Service (Bulletproof Hosting)
- direkter Zugriff auf Programme und Daten mit einem Browser
- Diese Vorteile haben jetzt auch Kriminelle für sich entdeckt und so ein neues Geschäftsmodell entwickelt

Ransomware as a Service (RaaS)

- damit kann sich jeder seinen individuell angepassten Erpressertrojaner im Netz zusammenstellen und anschließend verbreiten
- eigene Programmierkenntnisse sind damit unnötig
- es gibt neben dem eigentlichen Schädling auch Funktionen wie eine Übersicht der Zahlungseingänge und der Transaktionen & technischen Kundenservice
- vergütet werden die Dienste über eine Gewinnbeteiligung

=> je mehr Infektionen erfolgreich sind, umso höher die Ausschüttung an den "Kunden"

- Zahlungen erfolgen über Bitcoin – ein dezentrales, nicht-nachverfolgbares Währungssystems

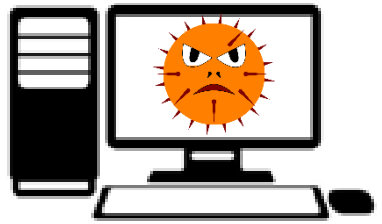
klopfer
datennetzwerk gmbh

- Ransomware bleibt wachsende Bedrohung
- klassischer Virenschutz ist nicht mehr ausreichend
- im Internet der Dinge (IoT) lauern weitere Bedrohungen
- Zunahme hoch automatisierter Angriffe
- Gefahren und Bedrohungen werden zunehmend professioneller
- Kritische Infrastrukturen (KRITIS) im Fadenkreuz

klopfer
datennetzwerk gmbh

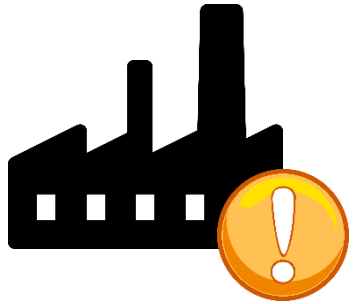
850 Mio. USD wurden **2016** für Ransomware-Angriffe gezahlt

Jeden Monat werden **30.000 - 50.000** Geräte mit Ransomware infiziert



Weniger als **25%** der Unternehmen informieren über einen Angriff

63% der Unternehmen verzeichneten **geschäftsbedrohende** Ausfallzeiten



klopfer
datennetzwerk gmbh

Backup

arcserve

IT-Security

SOPHOS