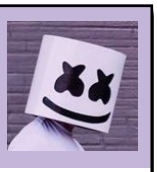
Technische und organisatorische Sicherheitsmaßnahmen

Praktische IT

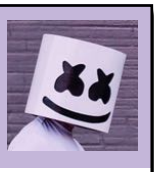
Robert Dorsch

IT-Sicherheit



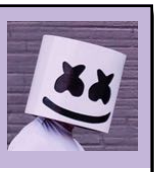
- Woran erkennen Unternehmen, dass sie angegriffen worden sind?
- Woran können sie erkennen, ob der Angreifer sich noch im Netz befindet?
- Wie erfahren Unternehmen, was der Angreifer im Netz tut (oder schon getan hat)?
- Was muss/kann ich jetzt tun?

Anlage § 9 BDSG



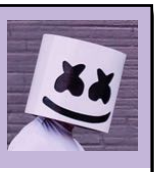
- *(Organisationskontrolle)*
- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungskontrolle

Lösungsansätze



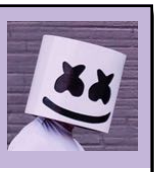
- Eine wirtschaftlich vernünftige und technisch schlagkräftige Abwehr ist nicht ohne ganzheitlichen Security-Ansatz realisierbar.
- Anlage zum § 9 BDSG muss Teil der IT-Sicherheitsstrategie werden.
- Technische Sicherheitssystem müssen mitwachsen.
- Vorhandenes Notfallmanagement unabdingbar.
  - - Geschäftsfortführungsplan
  - - Notfallvorsorgekonzept (präventiv)
  - - Notfallhandbuch (operativ)
  - - Sofortmaßnahmen

Zugangskontrolle



Nr.	Vorgabe	erfüllt	nicht erfüllt	nicht erforderlich	Bemerkungen
3.1	**Passwortverfahren**				
3.1.1	Forderung einer unterschiedlichen Zeichenzusammensetzung				Groß- und Kleinschreibung, Zahlen, Sonderzeichen
3.1.2	Mindestlänge 8 Zeichen				besser: länger als 16 Zeichen (z.B. ein einfach zu merkender Satz)
3.1.3	Regelmäßiger Wechsel				
3.1.4	Erstanmeldeprozedur				Vergabe des ersten Passwortes durch wen? Aufforderung/Prüfung der Änderung
3.1.5	Bildschirmsperre bei Pausen mit Passwort-Aktivierung				
3.1.6	Zugangssperre bei mehr als 3 Anmeldeversuchen				Protokollierung fehlerhafter Anmeldeversuche? Auswertung wann durch wen?
3.1.7	Passworthistorie				
3.1.8	Verwendung Gruppen-Passwörter				Sollte aufgrund der Nachvollziehbarkeit von Zugriffen unbedingt vermieden werden
3.1.9	Richtlinie, Merkblatt				
3.1.10	Aufbewahrung Administrator-Passwörter				Zugriffsregelungen?
3.1.11	Einmal-Passwörter				Software-/Hardware-Token?
3.1.12	BIOS-Passwörter				
3.1.13	Boot-Passwörter				
3.1.14	Single-Sign-On (SSO)?				
3.2	**Andere Verfahren**				
3.2.1	Biometrische Verfahren (one-to-one)				
3.2.2	Biometrische Verfahren (one-to-many)				
3.2.3	Elektronische Signatur				
3.2.4	Chipkarten				PIN-Vergabe und -Änderung?
3.2.5	Magnetkarten				
3.2.6	Transponderkarten				

NAC



Netzzugangskontrolle

Häufig ungesicherte Zugänge bei Unternehmen.

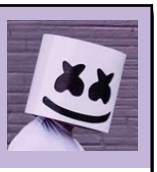
Bieten damit direkte Angriffsmöglichkeit auf geswitchte Netzwerke, DNS- oder DHCP-Protokolle.

Einfache Form der Netzzugangskontrolle sind White-List-Prüfungen.

NAC sind portbasierte Authentifizierungsmethoden, die die Verfügbarkeit und Funktionalität vom angeschlossenen Teilnehmer abhängig machen.

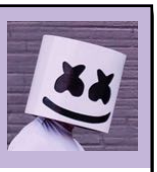
Damit lassen sich Netzteilnehmer direkt vom aktiven Netzwerk entkoppeln oder, den firmeninternen Sicherheitsrichtlinien entsprechend, in bestimmte VLANs einordnen.

Firewall



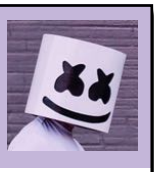
- Ein Großteil der Datenübertragungen per HTTP wird über Port 80 beziehungsweise per HTTPS über Port 443 abgewickelt
- Dieser kommt sowohl beim Surfen im Internet zum Einsatz, als auch zum Übertragen von Daten zu Cloud-Diensten wie Dropbox, zum Kommunizieren über WhatsApp oder auch zum Zugriff auf Office 365.
- Die Datenübertragungen dienen aber alle völlig unterschiedlichen Zwecken, sehen für eine traditionelle Firewall aber alle gleich aus.
- Sofern man eine Datenübertragung via HTTPS und Port 443 zulässt, so erlaubt die Firewall hierüber grundsätzlich alles, also auch die Übertragung infizierter Inhalte.

Firewall



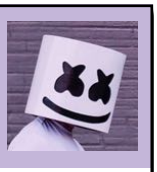
- Diese Vorgehen reichen inzwischen nicht mehr aus, um Unternehmensnetze sinnvoll gegen moderne Bedrohungslagen abzusichern.
- Grund dafür sind moderne Angriffsszenarien, wie beispielsweise verschlüsselte Datenübertragungen und APTs (Advanced Persistent Threats = *fortgeschrittene, andauernde Bedrohung*).
- APT bezeichnet einen komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten.
- Ziel eines APT ist es, möglichst lange unentdeckt im Netz zu bleiben, um über einen längeren Zeitraum an sensible Informationen zu kommen.

Next Generation Firewall



- Sicherheitslösungen, die über die reine Protokoll- und Portanalyse klassischer Firewalls hinausgehen und Datenanalysen auf Anwendungsebene ermöglichen.
- Next Generation Firewallsysteme untersuchen nicht nur das verwendete Protokoll und den eingesetzten Port, sondern auch den Inhalt des Datenstroms und erkennen ungewöhnliches Verhalten und filtern infizierte Dateien aus.
- Der Paketfilter wird dabei eng mit einem IDS kombiniert.

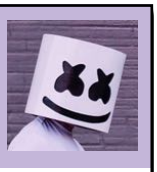
IDS/IPS Systeme

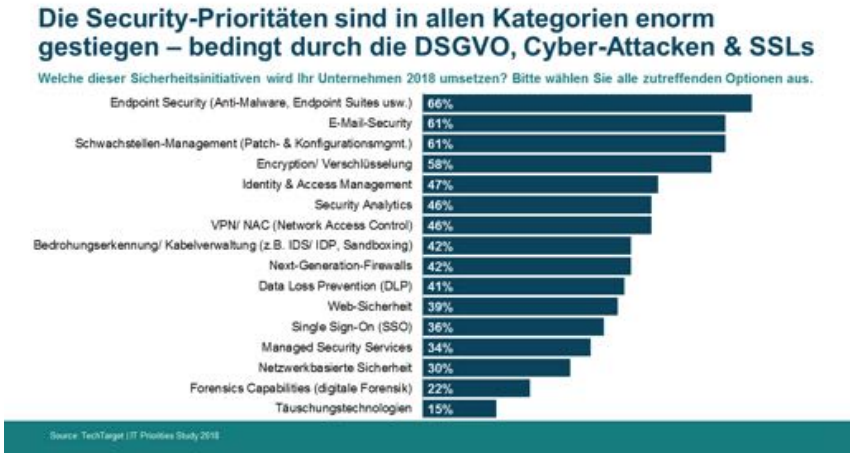


- IDS (Intrusion Detection System) Angriffserkennungssystem
- IDS-Verfahren verwenden Sensoren resp. Sniffer, die anormalen Datenverkehr aufspüren, mit vorgegebenen Mustern vergleichen und einen Alarm auslösen.

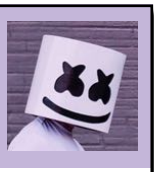
- IPS (Intrusion Prevention System) Angriffsabwehrsystem
- IPS erkennt Bedrohungen, arbeitet aber aktiv und ergreift selbständig Maßnahmen zum Schutz des LAN, Beispielsweise den Verkehr von einer bestimmten Quelle blockieren.

Verschiebung der IT-Budgets

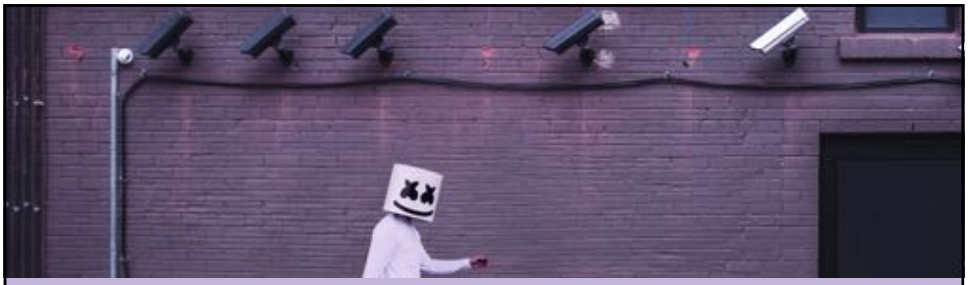




Fazit



- IT-Sicherheit lässt sich nur bedingt kaufen.
- Ohne grundlegenden IT-Sicherheitsprozess bleibt der Informationsverbund verwundbar.
- umfassendes Identity-Management (IdM).
- Effektive Schutzmaßnahmen für Maschinenidentitäten verlangen vollständige Sichtbarkeit und eine kontinuierliche Beobachtung aller Identitäten.
- Gezielte Angriffe erfordern mehrstufigen Schutz und intelligente Sicherheit auf allen Endgeräten.



DS2018 Gesellschaft für Datenschutz und Datensicherheit GmbH

Sommerbergstraße 97
66346 Püttlingen
Regionalverband Saarbrücken
Telefon 06806/4999529
Telefax 06806/920294
E-Mail info@ds2018.de