Entdecken Sie neue Wege im Kampf gegen Cyberkriminelle

Sebastian Haacke
Sales Engineer

SOPHOS

ito consult GmbH

UTMshop

- Gründung 21 Jahren - seit 15 Jahren SOPHOS (vormals ASTARO) Partner
- strikte Fokussierung auf Sophos
- Sophos Platinum Partner mit vielen hundert Kunden in ganz Deutschland (und DACH)
- spezialisierte und zertifizierte Techniker und Vertriebsmitarbeiter die für alle Fragen zum Thema Sophos zur Verfügung stehen

Sophos – mehr als 30 Jahre Erfahrung

1985 GRÜNDUNG OXFORD, UK

630M UMSATZ (FY17)

3.000 MITARBEITER

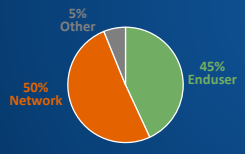
400 in DACH

HQ ABINGDON, UK

200,000+ KUNDEN

100M+ ANWENDER

20,000+ CHANNEL PARTNER



- Akquisition u.a. von Utimaco 2009, Astaro 2011, Dialogs 2012, Cyberoam 2014, Mojave 2014, Reflexion 2015, SurfRight 2015, Barricade 2016, Invincea 2017
- Gartner: Marktführer in den Bereichen Endpoint, Verschlüsselung & UTM

SOPHOS

Gartner Leader in Endpoint, UTM und Verschlüsselung

Gartner Magic Quadrant ENDPOINT PROTECTION

Magic Quadrant for Endpoint Protection Platforms, Eric Ouellet, Ina McShane, Avivah Litan 30 January, 2017

Gartner Magic Quadrant UNIFIED THREAT MANAGEMENT

Magic Quadrant for Unified Threat Management, Jeremy D'Hoinne, Adam Hils, Rajpreet Kaur, 30 August, 2016

Gartner Magic Quadrant MOBILE DATA PROTECTION

Magic Quadrant for Mobile Data Protection, John Girard, 8 October, 2015

SOPHOS

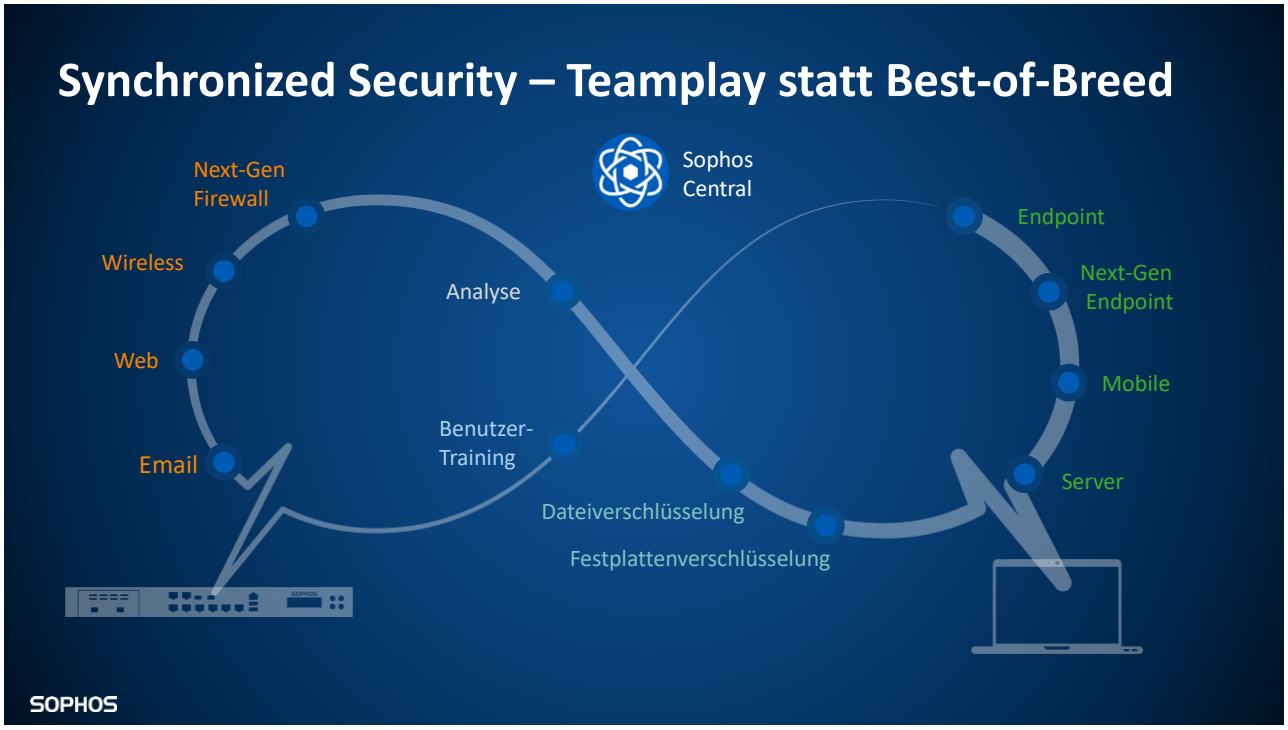
Was ist Synchronized Security?

Synchronized Security

SOPHOS

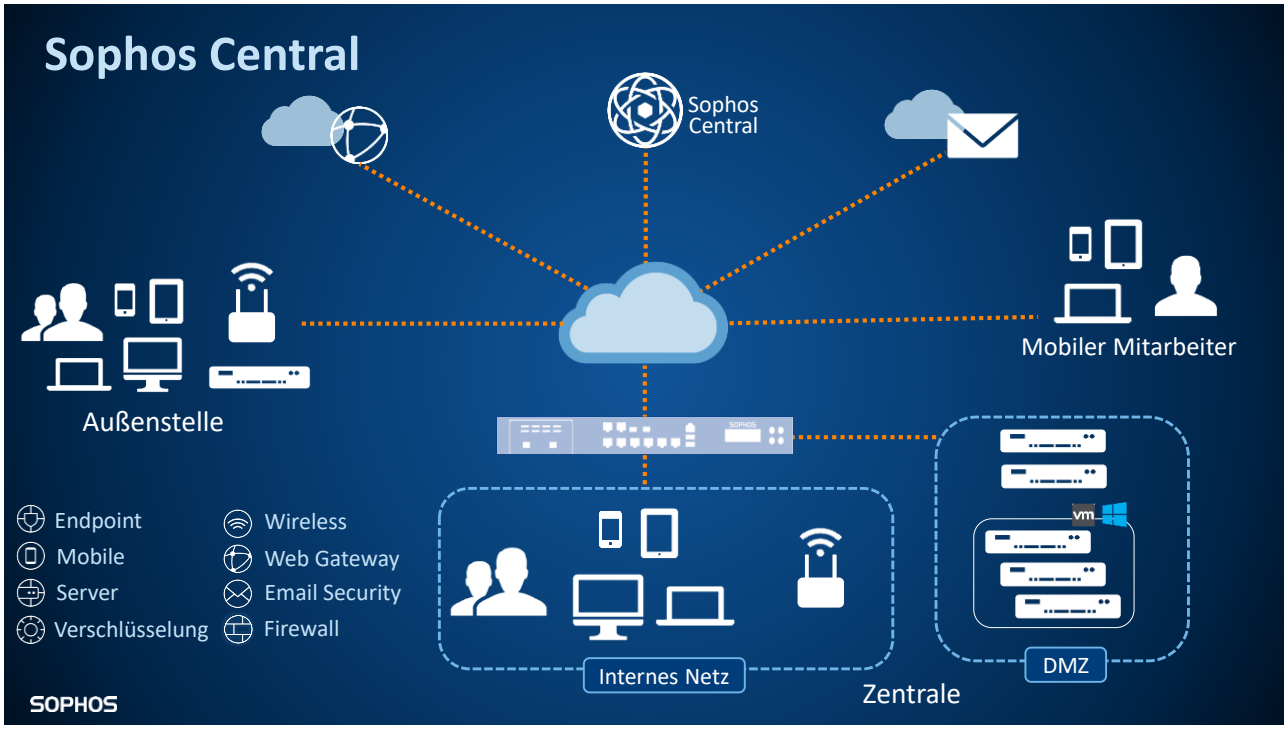
Ein Beispiel


IT Security
Traditionelle Security
NextGen Security
Einfaches Management
Synchronized Security
Security Heartbeat
Anti-Virus
LiveProtection & HIPS
Web Control
Device Control
Application Control
Whitelisting
Komplette Security in einer Oberfläche
Sofort startbereit
Ursachenanalyse
Machine Learning
Verhaltenserkennung
Exploit Prevention
SOPHOS
Security made simple.
SOPHOS


Synchronized Security – Teamplay statt Best-of-Breed
Sophos Central
Next-Gen Firewall
Wireless
Web
Email
Analyse
Benutzer-Training
Endpoint
Next-Gen Endpoint
Mobile
Server
Dateiverschlüsselung
Festplattenverschlüsselung
SOPHOS

Sophos Central

SOPHOS



Warum waren die Krypto-Trojaner so erfolgreich?

SOPHOS

Gründe für Infektionen trotz Best-of-Breed Security

- Office-Dokumente und PDFs in E-Mails oft zugelassen
- Technologisch fortgeschrittene Schädlinge
- Hochprofessionelle Angreifer
- Geschicktes Social Engineering
- Sicherheitssysteme fehlen oder falsch konfiguriert
- Sicherheitssysteme agieren nicht als System

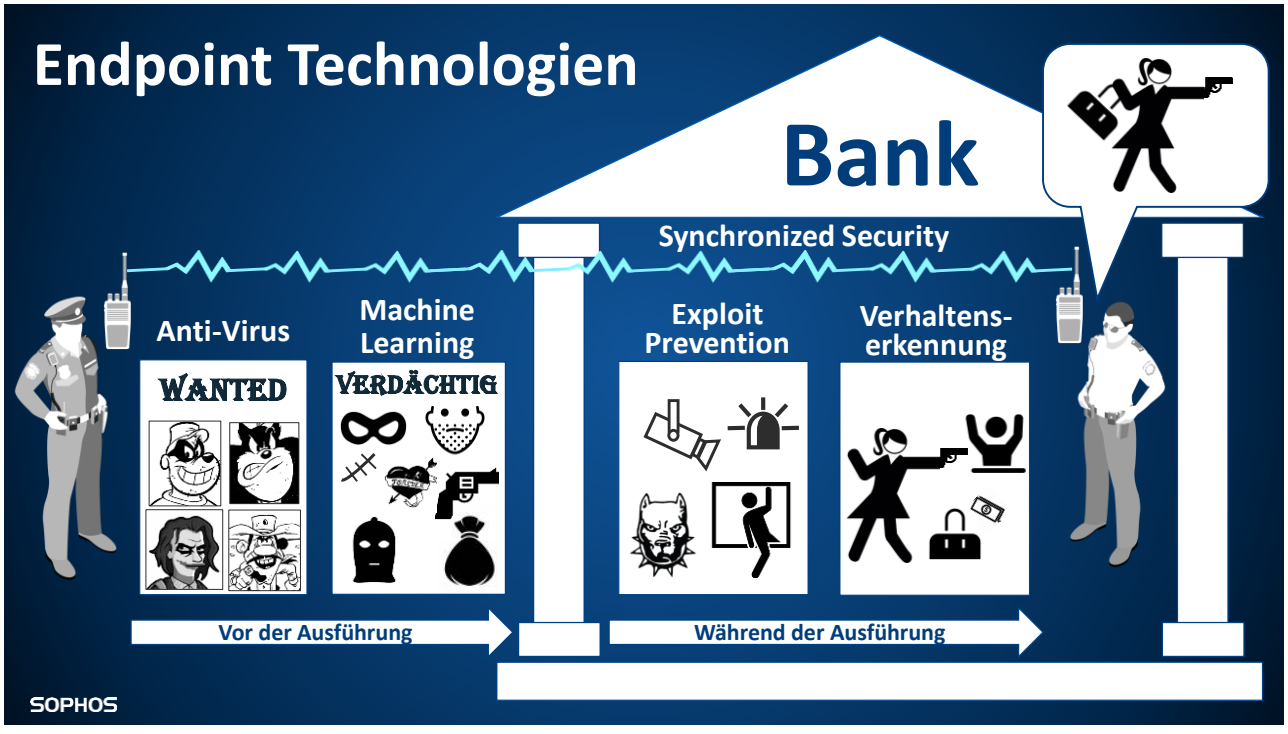

Betreff: Offizielle Warnung vor Computervirus Locky

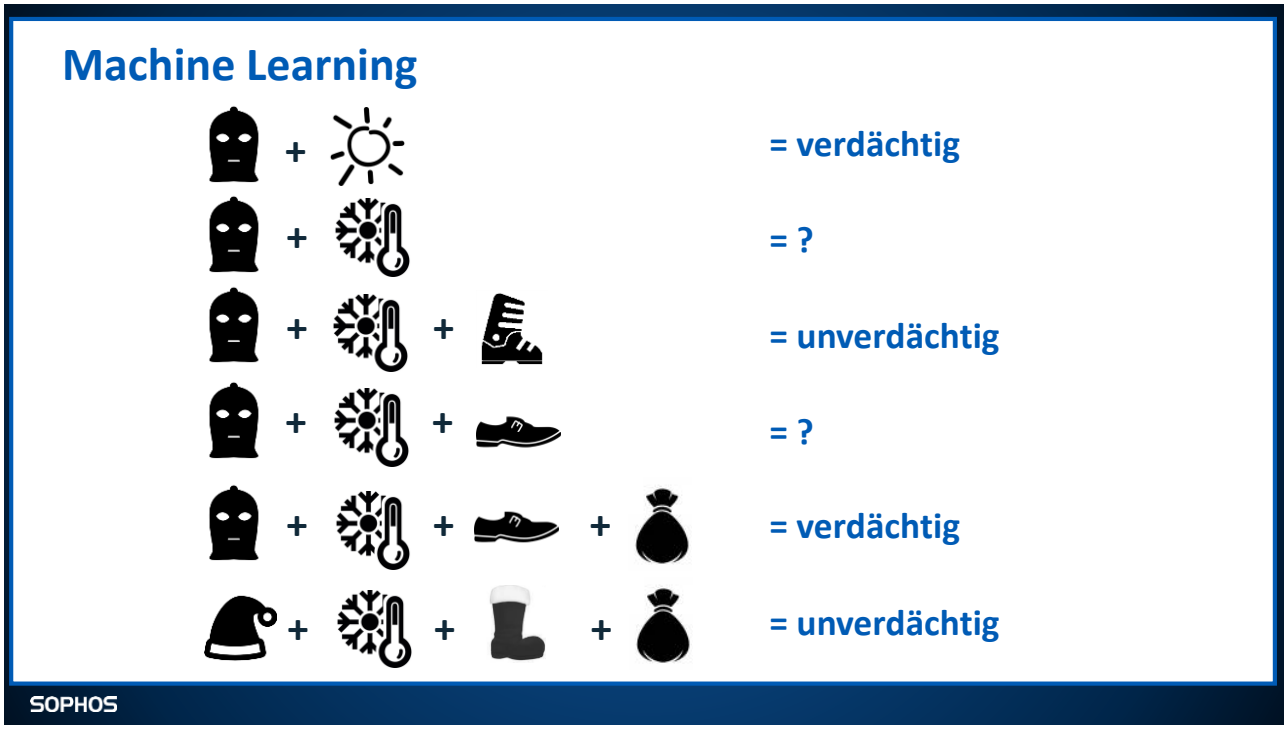
Bundeskriminalamt

Offizielle Warnung vor Computervirus Locky

Aufgrund wiederholter Email mit Nachfragen wie man sich im Falle einer
Infektion mit dem Computervirus "Locky" zu verhalten hat, haben Wir uns dazu entschieden in Ko
mit Anti Virensoftware Herstellern einen Sicherheitsratgeber zu Verfügung

SOPHOS


Endpoint Technologien
Bank
Synchronized Security
Anti-Virus
WANTED
Machine Learning
VERDÄCHTIG
Exploit Prevention
Verhaltens-erkennung
Vor der Ausführung
Während der Ausführung
SOPHOS


Machine Learning
= verdächtig
= ?
= unverdächtig
= ?
= verdächtig
= unverdächtig
SOPHOS

Grenzen von Machine Learning

Sehr effektiv bei Programmdateien

..aber – nur 56% aller Malware kommt als Programmdatei, die von Machine Learning untersucht werden kann

Dateibasierte Malware

Programmdateien	Dokumente und Mediendateien	Scripts, Java, Webseiten	Sonstige
56%	30%	11%	3%

SOPHOS

Wo Malware heute am Endpoint aufgehalten wird

400.000 neue Schädlinge / Tag

80%	15%	3%	2%
Einfallsweg schließen	**Analyse vor Ausführung**	**Exploit-Vehinderung**	**Verhaltens-Erkennung**
• URL-Filterung • Download Reputation • Device Control • App Control	• Signaturen • Heuristiken • Machine Learning	• Einbruchstechniken erkennen/verhindern • Rechteausweitung verhindern	• Verschlüsselung • Hacker-Aktivität • Passwort- und Datendiebstahl

SOPHOS

Sophos INTERCEPT X



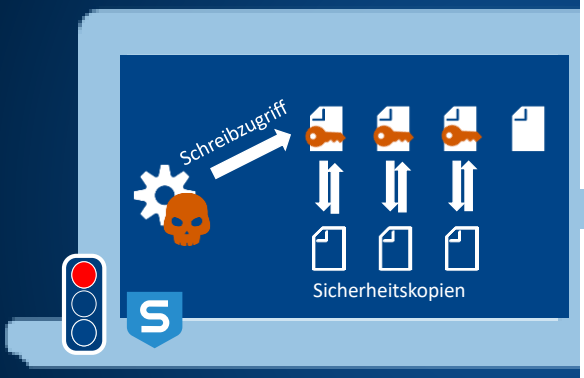

Anti-Ransomware	*Anti-Exploit*	*Erweiterte Bereinigung*	*Ursachenanalyse*
Stoppt Krypto-Trojaner • Erkennt und verhindert Verschlüsselung • Stellt Originaldateien wieder her	**Stoppt unbekannte Malware** • Signaturloser Schutz vor Zero-Day-Angriffen • Keine Performanceeinbußen	**Entfernt die Bedrohung** • Signaturlose Erkennung und Entfernung von bisher unbekannter Malware	**Analysiert den Angriff** • Was ist passiert? • Was ist gefährdet? • Wie verhindere ich das zukünftig?

SOPHOS

Anti-Ransomware

SOPHOS

CryptoGuard - lokale Ransomware



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	7B	5C	72	74	66	31	5C	61	6E	73	69	5C	61	6E	73	69	{\rtf1\ansi\ansi
00000010	63	70	67	31	32	35	32	5C	64	65	66	66	30	5C	64	65	cpg1252\deff0\de
00000020	66	6C	61	6E	67	31	30	34	33	7B	5C	66	6F	6E	74	74	flang1043{\fontt
00000030	62	6C	7B	5C	66	30	5C	66	6E	69	6C	5C	66	63	68	61	bl{\f0\fnil\fcha
00000040	72	73	65	74	30	20	56	65	72	64	61	6E	61	3B	7D	7D	rset0 Verdana;}}
00000050	5C	72	5C	6E	5C	76	69	65	77	6B	69	6E	64	34	5C	75	\r\n\viewkind4\u
00000060	63	31	5C	70	61	72	64	5C	73	61	32	30	30	5C	73	6C	c1\pard\sa200\sl
00000070	32	37	36	5C	73	6C	6D	75	6C	74	31	5C	6C	61	6E	67	276\slmult1\lang
00000080	39	5C	66	30	5C	66	73	32	32	20	54	68	65	20	71	75	9\f0\fs22 The qu
00000090	69	63	6B	20	62	72	6F	77	6E	20	66	6F	78	20	6A	75	ick brown fox ju
000000A0	6D	70	73	20	6F	76	65	72	20	74	68	65	20	6C	61	7A	mps over the laz
000000B0	79	20	64	6F	67	2E	7D										y dog.}

Unverschlüsselte Datei vor Schreibvorgang

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	7D	EB	10	B2	FD	8E	EB	B9	D1	F6	D8	DE	CC	9B	F6	CB	}ë.²ýŽë¹ÑöØÞÌ›öË
00000010	C4	D9	C3	F6	CB	C4	D9	C3	C9	DA	CD	9B	98	9F	98	F6	ÄÙÃöËÄÙÃÉÚÍ›˜Ÿ˜ö
00000020	CE	CF	CC	CC	9A	F6	CE	CF	CC	C6	CB	C4	CD	9B	9A	9E	ÎÏÌÌšöÎÏÌÌÆËÄÍ›šž
00000030	99	D1	F6	CC	C5	C4	DE	DE	C8	C6	D1	F6	CC	9A	F6	CC	™ÑöÌÅÄÞÞÈÆÑöÌšöÌ
00000040	C4	C3	C6	F6	CC	C9	C2	CB	D8	D9	CF	DE	9A	8A	FC	CF	ÄÃÆöÌÉÂËØÙÏÞšŠüÏ
00000050	D8	CE	CB	C4	CB	91	D7	D7	F6	D8	F6	C4	F6	DC	C3	CF	ØÎËÄË'××øØöÄöÜÃÏ
00000060	DD	C1	C3	C4	CE	9E	F6	DF	C9	9B	F6	DA	CB	D8	CE	F6	ÝÁÃÄÎžößÉ›öÚËØÎö
00000070	D9	CB	98	9A	9A	F6	D9	C6	98	9D	9C	F6	D9	C6	C7	DF	ÙË˜šš öÙÆ˜.œöÙÆÇß
00000080	C6	DE	9B	F6	C6	CB	C4	CD	93	F6	CC	9A	F6	CC	D9	98	ÆÞ›öÆËÄÍ"öÌšöÌÙ˜
00000090	98	8A	FE	C2	CF	8A	DB	DF	C3	C9	C1	8A	C8	D8	C5	DD	˜ŠþÂÏŠÛßÃÉÁŠÈØÅÝ
000000A0	C4	8A	CC	C5	D2	8A	C0	DF	C7	DA	D9	8A	C5	DC	CF	D8	ÄŠÌÅÒŠÀßÇÚÙŠÅÜÏØ
000000B0	8A	DE	C2	CF	8A	C6	CB	D0	D3	8A	CE	C5	CD	84	D7		ŠÞÂÏŠÆËÐÓŠÎÅÍ„×

Verschlüsselte Datei nach Schreibvorgang

Ursachenanalyse

Erweiterte Bereinigung mit Sophos Clean

SOPHOS

Wo lauert die größere Gefahr?

SOPHOS

Anti-Exploit

SOPHOS

Schutz vor unbekannter Malware über Exploit-Prevention

Neue Malware-Varianten pro Jahr

100,000,000+

Exploit-Techniken

Etwa 1 neue Exploit-Technik pro Jahr, ~25 Techniken existieren insgesamt.

- Stack Pivot
- Buffer Overflow
- Branch-based ROP Mitigations (Hardware Augmented)
- Null Page (Null Dereference Protection)
- Bottom Up ASLR
- Reflective DLL Injection
- Stack-based ROP Mitigations (Caller)
- Dynamic Heap Spray
- Heap Spray Allocation
- Application Lockdown
- APC Violation
- Load Library
- Stack Exec (MemProt)
- Hollow Process
- Java Lockdown
- DLL Hijacking
- Squiblydoo AppLocker Bypass
- VBScript God Mode
- Import Address Table Filtering (IAF) (Hardware Augmented)
- Syscall
- WoW64
- Mandatory Address Space Layout Randomization (ASLR)
- Structured Exception Handler Overwrite Protection (SEHOP)

SOPHOS

Schon jetzt beste Exploit-Erkennung am Markt

SOPHOS

Exploits unter der Lupe:

Welche Security-Produkte wehren Exploits zuverlässig ab?

Exploits nutzen Schwachstellen in legitimen Software-Produkten wie Adobe Flash und Microsoft Office aus, um Computer für kriminelle Zwecke zu infizieren. Häufig werden sie von Cyberkriminellen genutzt, um die Abwehrmaßnahmen von Unternehmen zu überlisten. Die Beweggründe dieser Kriminellen sind vielfältig: Manche wollen Daten stehlen oder Lösegeld für die Herausgabe von Daten erpressen, andere Informationen über ihr Ziel sammeln oder einfach nur mehr gewöhnliche Malware in Umlauf bringen.

Exploits werden häufig im Rahmen von Cyberangriffen verwendet: Bei über 90 % aller gemeldeten Datenpannen kann der Einsatz eines Exploits an einem oder mehreren Punkten der Angriffskette nachgewiesen werden. Eine Exploit Prevention darf also in keiner umfassenden Sicherheitslösung fehlen.

Exploits gibt es schon seit mehr als 30 Jahren. Kein Wunder also, dass die meisten IT-Security-Anbieter die eine oder andere Form der Exploit Prevention im Angebot haben. Die Qualität dieser Exploit Prevention kann jedoch stark variieren. Für einige Anbieter ist Exploit Prevention eine reine Pflichtübung, für andere wiederum ein wichtiger strategischer Schwerpunkt. In diesem Whitepaper erfahren Sie mehr über Exploits und welche Exploit-Prevention-Funktionen die führenden Security-Produkte zu bieten haben.

	Sophos Intercept X	ESET Endpoint Security	Kaspersky Endpoint Security	McAfee Endpoint Security	Symantec Endpoint Protection	Trend Micro OfficeScan	Webroot Endpoint Protection	CylancePROTECT	Microsoft EMET	Malwarebytes Anti-Exploit	Palo Alto Networks Traps	CrowdStrike Falcon
Enforce Data Execution Prevention (DEP) Unterbindet die missbräuchliche Nutzung von Pufferüberläufen	▪			▪					▪	▪	▪	▪
Mandatory Address Space Layout Randomization (ASLR) Verhindert vorhersagbare Code-Speicherorte	▪								▪1		▪	▪1
Bottom Up ASLR Optimiert die Randomisierung von Code-Speicherorten	▪								▪	▪		
Null Page (Null Dereference Protection) Stoppt Exploits, die Sprungbefehle über die Zero-Page beinhalten	▪		▪						▪			
Heap Spray Allocation Reserviert beim Programmstart Speicherbereiche, die häufig für das Einbringen von Schadcode verwendet werden, um solche Angriffe abzuwehren	▪				▪				▪	▪	▪	▪
Dynamic Heap Spray Stoppt Angriffe, die verdächtige Sequenzen an verschiedene Stellen des Heaps schreiben	▪										▪2	
Stack Pivot Stoppt missbräuchliche Nutzungen des Stack Pointers	▪			▪		▪		▪	▪	▪	▪	
Stack Exec (MemProt) Stoppt Code von Angreifern auf dem Stack	▪					▪		▪	▪			
Stack-based ROP Mitigations (Caller) Stoppt „Return-Oriented Programming"-Standardangriffe	▪		▪3	▪1		▪			▪	▪	▪	
Branch-based ROP Mitigations (Hardware Augmented) Stoppt komplexe „Return-Oriented Programming"-Angriffe	▪											
Structured Exception Handler Overwrite Protection (SEHOP) Stoppt missbräuchliche Nutzungen des Ausnahmehandlers	▪				▪4				▪2			

	Sophos Intercept X	ESET Endpoint Security	Kaspersky Endpoint Security	McAfee Endpoint Security	Symantec Endpoint Protection	Trend Micro OfficeScan	Webroot Endpoint Protection	CylancePROTECT	Microsoft EMET	Malwarebytes Anti-Exploit	Palo Alto Networks Traps	CrowdStrike Falcon
Import Address Table Filtering (IAF) (Hardware Augmented) Stoppt Angriffe, die nach API-Adressen in der IAT suchen	▪								EAF, EAF+			
Load Library Unterbindet das Laden von Libraries von UNC-Pfaden	▪								▪	▪	▪	
Reflective DLL Injection Verhindert das Laden einer Library vom Speicher in einen Host-Prozess	▪										▪	
VBScript God Mode Verhindert die Ausnutzung von VBScript in IE zur Ausführung von Schadcode	▪								▪	▪	▪5	
WoW64 Stoppt Angriffe, die auf die 64-Bit-Funktion des WoW64-Prozesses abzielen	▪											
Syscall Stoppt Angreifer, die versuchen, Sicherheitsmaßnahmen zu umgehen	▪											
Hollow Process Stoppt Angriffe, die legitime Prozesse nutzen, um Schadecode zu verbergen	▪										▪	
DLL Hijacking Gibt System-Libraries für heruntergeladene Anwendungen Priorität	▪											
Application Lockdown Stoppt Logic-Flaw-Angriffe, die Abwehrmaßnahmen umgehen	▪									▪	▪1	
Java Lockdown Verhindert Angriffe, die Java ausnutzen, um ausführbare Windows-Dateien zu starten	▪									▪	▪	
Squiblydoo AppLocker Bypass Verhindert die Ausführung von Remote-Skripte und -Code durch regsvr32	▪				▪							
CVE-2013-5331 & CVE-2014-4113 via Metasploit In-Memory Payloads: Meterpreter & Mimikatz	▪	▪	▪						▪		▪	

SOPHOS

Ursachen-Analyse

SOPHOS

Ursachenanalyse

Was ist passiert?

Analyse des Vorfalls

- Identifikation betroffener Prozesse, Registry-Keys, Dateien, Kommunikation
- Grafische Darstellung der Ereigniskette
- Eintrittspunkte der Malware ins Netzwerk

Was ist gefährdet?

Betroffene Ressourcen

- Welche Dateien und Systeme sind betroffen?
- Auf welche Netzlaufwerke oder Wechselmedien wurde zugegriffen?
- Welche Systeme muss ich noch bereinigen?

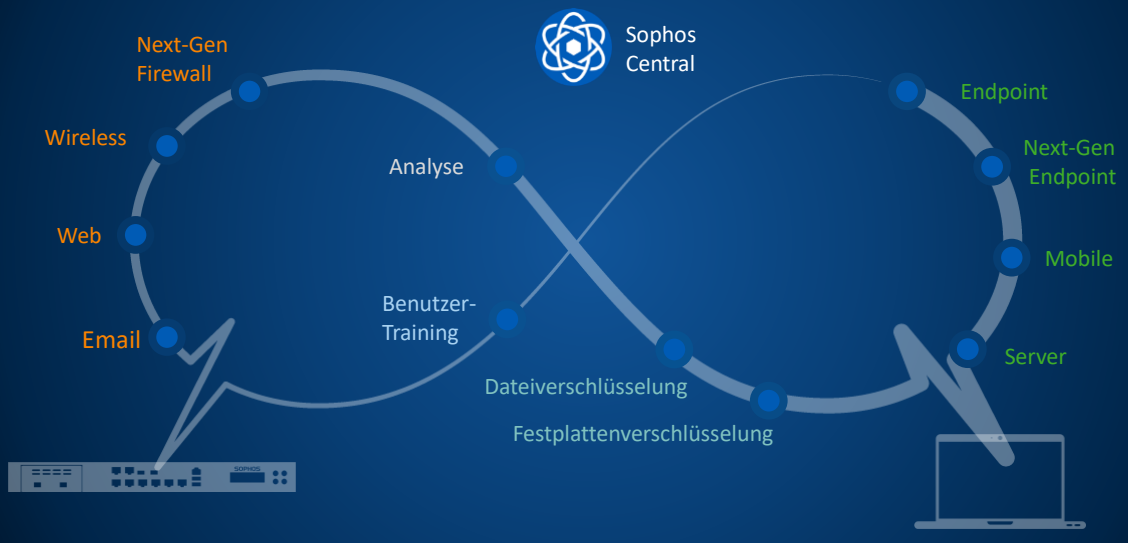
Wie verhindere ich das zukünftig?

Konsequenzen

- Welche Einfallswege für Malware muss ich schließen?
- Wie kann ich eine Verbreitung im Netzwerk zukünftig verhindern?

SOPHOS

Synchronized Security – Teamplay statt Best-of-Breed

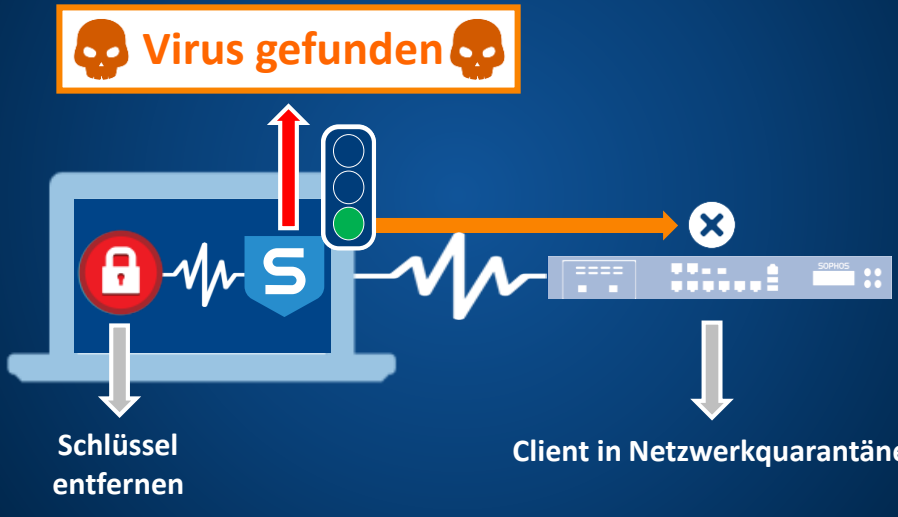


SOPHOS

Security Heartbeat

SOPHOS

Security Heartbeat - Vireninfektion



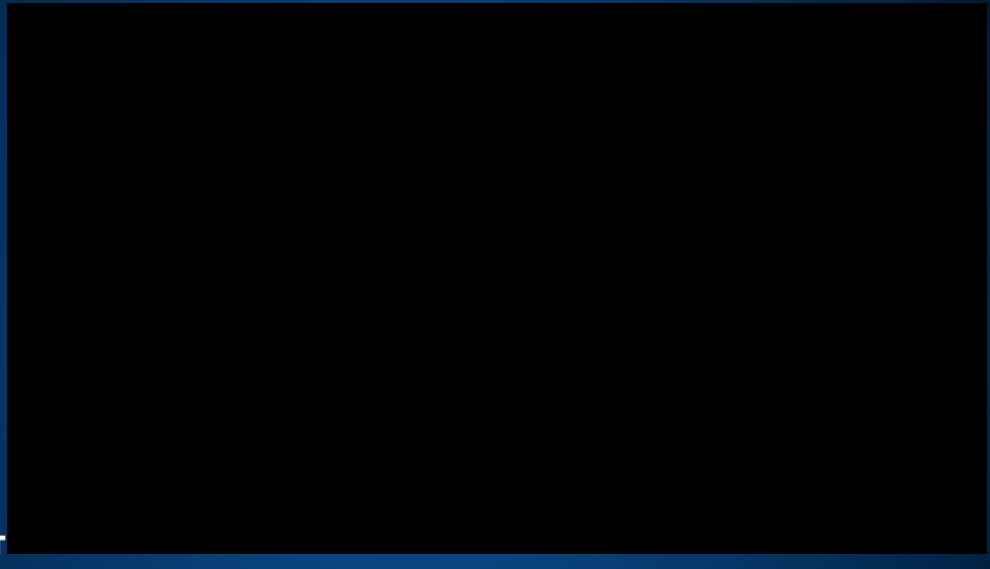
SOPHOS

Demo

INTERCEPT X

Synchronized Security

SOPHOS



Demo

INTERCEPT X

Synchronized Security

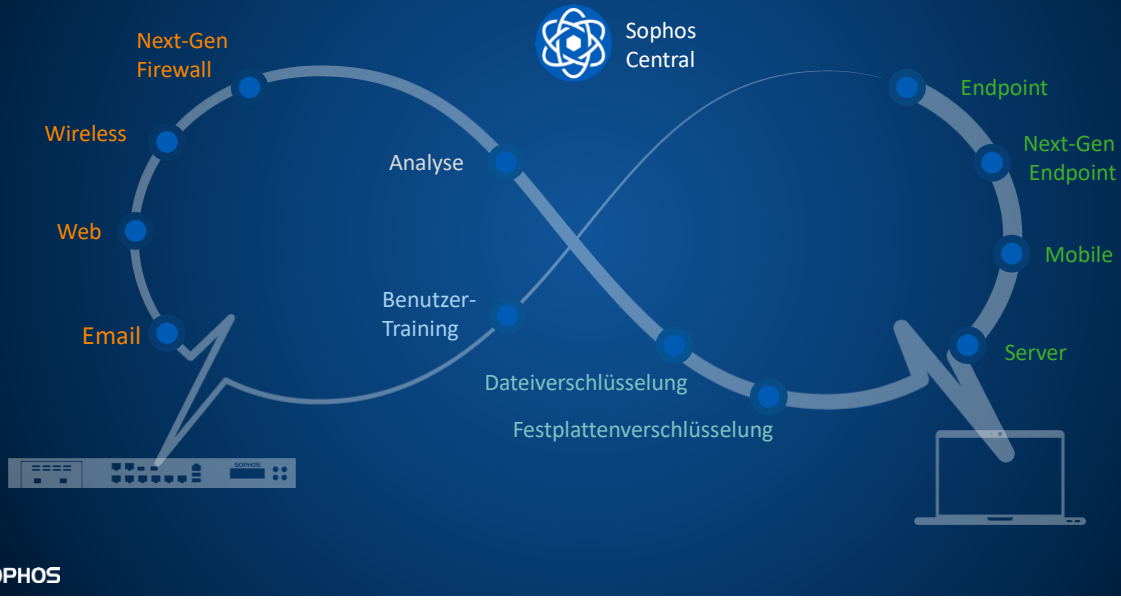
SOPHOS

Finale Verteidigungslinie
Sicherheit als System

Synchronized Security

SOPHOS

Synchronized Security – Teamplay statt Best-of-Breed



SOPHOS


SOPHOS
Security made simple.