Ransomware

Jos Oostdam
8 december 2021

kpn. Het netwerk van Nederland

Jos Oostdam

Warming up

Wat hebben de Zweedse supermarktketen Coop, het Amerikaanse Colonial Pipeline en Braziliaanse vleesverwerker JBS met elkaar gemeen?

Hoeveel verschillende ransomware families zijn er geïdentificeerd?

Waar vind je gratis decryptiesoftware voor ruim 150 verschillende typen ransomware?

Bronnen: https://www.kpn.com/zakelijk/blog/kpn-security-helpt-fbi-ransomware.htm, Verkeersnet.nl, https://www.nomoreransom.org/nl/index.html

Ransomware Bingo

Crimineel	Volwassen	Verdienmodel
Losgeld	Dienstverlening	Internationaal
Kill chain	Supply chain	Weerbaarheid

Source: Cybersecuritybeeld Nederland 2021. NCTV, https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

NIST Framework

Bron: NIST, Framework for Improving Critical Infrastructure Cybersecurity. NIST, version 1.1, 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Identify

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management

Hardware, software, netwerk

Classificatie klanten, diensten, gebouwen, applicaties etc

Business continuïteitseisen

Wettelijke eisen en regelingen

Rollen, verantwoordelijkheden, mandaten (extern en intern)

Risicoanalyse, threat intel

Keteninzicht (extern en intern)

Contractafspraken

Ketenoefeningen en -testen

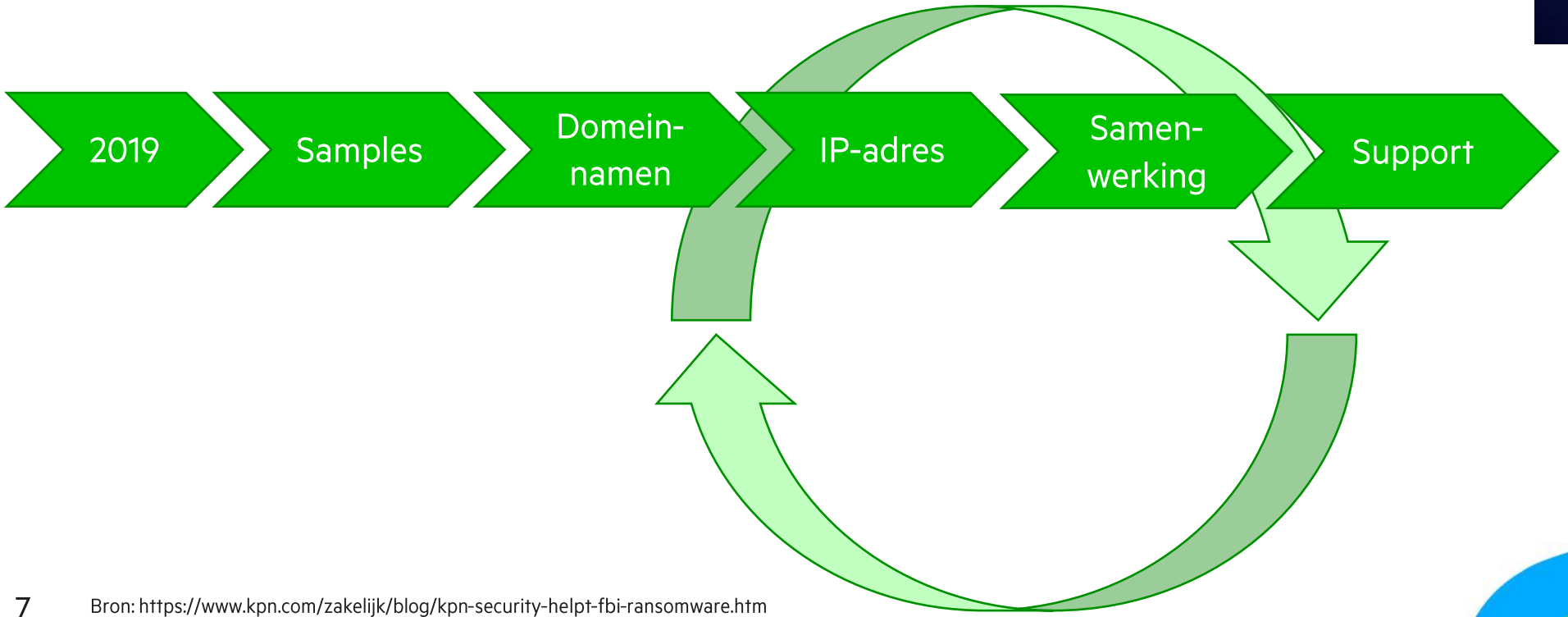
Bron: NIST, Framework for Improving Critical Infrastructure Cybersecurity. NIST, version 1.1, 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Internationale samenwerking

Home > Zakelijk > The Digital Dutch > Blog > **KPN Security helpt FBI bij strijd tegen ransomware**

KPN Security helpt FBI bij strijd tegen ransomware

26 november 2021



Bron: https://www.kpn.com/zakelijk/blog/kpn-security-helpt-fbi-ransomware.htm

Protect

Function Unique Identifier	Function	Category Unique Identifier	Category
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Fysieke en logische toegang, review

Persoonlijke accounts

End Point Protection

BCM, trainingen en testen

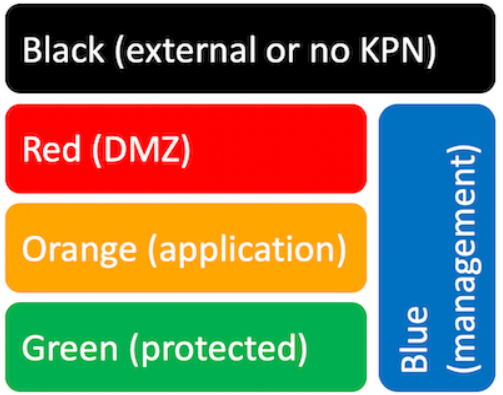
Data

Bedrijfscode, KPN Security Policy

Life Cycle Management

Vulnerability management

Log management



Bron: https://ciso-ksp.kpnnet.org/

Bron: NIST, Framework for Improving Critical Infrastructure Cybersecurity. NIST, version 1.1, 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Detect

Function Unique Identifier	Function	Category Unique Identifier	Category
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes

Security Information and Event Management (SIEM)

Security Orchestration, Automation, and Response (SOAR)

Forensische expertise

Werkplekken

Vulnerability management

MITRE | ATT&CK™

Bron: https://attack.mitre.org/

Bron: NIST, Framework for Improving Critical Infrastructure Cybersecurity. NIST, version 1.1, 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

kpn

Respond

Function Unique Identifier	Function	Category Unique Identifier	Category
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements

Centraal en specifiek meldpunt

Continuïteitsplannen

Be Alert incident management proces

Play books

Corporate Crisis Management Team (CCMT)

Externe stakeholders

Externe hulp

Documentatie

Evaluatie en updates

Bron: NIST, Framework for Improving Critical Infrastructure Cybersecurity. NIST, version 1.1, 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Recover

Function Unique Identifier	Function	Category Unique Identifier	Category
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Herstel prioriteiten

Backups

Communicatie

Bron: NIST, Framework for Improving Critical Infrastructure Cybersecurity. NIST, version 1.1, 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Ransomware related security controls

Level	Measure	Status
Identify	Asset Management	
Identify	Vulnerability Management	
Identify	Penetration testing	
Protect	Awareness & Training	
Protect	End Point Protection	
Protect	Identity and Access Management	
Protect	System Hardening	
Protect	Network segmentation	
Protect	Patch Management	
Detect	SIEM, Log Monitoring	
Respond	IT Security Incident Management	
Recover	Business Continuity Management	

Toekomst?

Kunstmatige intelligentie

Strafbaarstelling losgeld betaling

Focus op bescherming

Focus op voorkomen (wetshandhaving)

kpn. Het netwerk van Nederland