



Van wildgroei naar weerbaarheid

IT en OT veilig verbinden in organisaties

Michel van Eeten (TU Delft)

De digitale transformatie van het Europese energiesysteem versnellen

Information notification
Dit is een machinevertaling die door de Europese Unie wordt verstrekt. De dienst vertaling van de Commissie helpt u deze pagina te begrijpen. Alstublieft lees de oorspronkelijke versie te lezen, zie de brontekst

Interoperabele en open digitale oplossingen, evenals gegevenssoevereinheid, zijn essentieel voor de digitale transformatie van het energiesysteem.
Het verminderen van de uitstoot van broeikasgassen met 55 % en het aandeel van hernieuwbare energie in 2030 kan alleen gebeuren als het energiesysteem er klaar voor is.



Digitale transformatie

De wereld verandert en digitaliseert in rap tempo. Dit biedt kansen om dingen anders en slimmer te doen. Tegelijkertijd brengt het digitale tijdperk nieuwe risico's en dilemma's met zich mee en zijn we steeds afhankelijker van een goed functionerende ICT-infrastructuur en -dienstverlening.



ADVERTORIAL

Digitalisering in transport en logistiek: de weg naar efficiëntie

Gepubliceerd op 16-12-2024 om 09:11

• Alle sectoren digitaliseren
• Dat betekent: niet-IT wordt ook IT
• Verantwoordelijkheid blijft op dezelfde plek
• Ergo: veel medewerkers zijn de facto IT-beheerders geworden



NIEUWS

Boeren & data: biedt digitaliseringsvisie dé uitkomst?

Redactie Groen Kennisnet • 4 oktober 2021



Foto: Seeders

De transport- en logistieke sector staat voor een enorme kostenbesparing altijd centraal staan.



IT <> ~~OT~~

IT die door ~~is~~ iemand
andere is ingekocht
niet IT'er ←



centrum informatiebeveiliging
en privacybescherming

Whitepaper IoT II

Weerbaarheid in de praktijk

Over Internet of Things en veiligheid voor alle overheden

- “Julie hebben een kwetsbaar systeem verbonden aan een verkeersregelinstallatie”. Na uitzoekwerk: Deze is waarschijnlijk van de Provincie. Na uitzoekwerk van de Provincie: deze is waarschijnlijk van Rijkswaterstaat. Na uitzoekwerk van Rijkswaterstaat: deze is van een vierde partij die camerabeelden op een website zet.

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van onvolledigheid, onjuistheden en/of gebreken. Het is altijd de verantwoordelijkheid van de lezer zelf om te beoordelen en ingewoond te worden indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctievoorstellen en suggesties.



© Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamvermelding-GeenGeld 4.0 International (CC BY-NC 4.0) verleend. Voor meer informatie zie: <https://creativecommons.org/licenses/by-nc/4.0/>

→ cliffhanger!

“beheersvraagstuk”



klassieke reflex: centralisatie

← versterkt
door NIS2

“duidelijke kaders”

“control”

“compliance”

“heldere
verantwoordingslijnen”

digitaal / nieuws

Waarom security van sluizen en gemalen een zorgenkindje blijft

De IBD schakelt experts in om security van IACS bij gemeenten te verbeteren.

📄 Sjoerd Hartholt 📅 29 maart 2024

OT

hebben bij IACS en zij regelen vaak alles zelf. Er is vaak geen eenduidig beeld binnen de gemeente over de inzet van IACS, wie de eigenaar ervan is, hoe het beheerd wordt en tenslotte de beveiliging ervan.' Volgens de IBD is het essentieel om de controle van de security van IACS bij de CISO te beleggen.

Bijvoorbeeld: "Maak CISO verantwoordelijk"

Informatievoorziening

Functioneel Beneerder PP Apoyo

JS Consultancy

risico's van centralisatie



overbelasting IT-
security functie



Insights / Information Technology / Article

Cybersecurity Leaders Are Burned Out. Here's Why.

- Cybersecurity leaders face unique stressors, raising their risk of burnout.
- Gartner Peer Community surveyed 178 cybersecurity leaders to uncover the most common causes.


5 Most Common Causes of Burnout for Cybersecurity Leaders



Source: Gartner
© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. 2726926


Gartner
Peer Community™

risico's van centralisatie



overbelasting IT-
security functie

①



IT security is niet goed in
proportionele risico-
inschattingen buiten het eigen
domein

②

Tienduizenden verkeerslichten in Nederland te hacken, lek nog jaren te misbruiken

Door Daniël Verlaan · 5 oktober 2024 · Aangepast: 25 oktober 2024



Onderzoek

"Dit is een ernstige hack die de fysieke wereld kan manipuleren", zegt cybersecurity-expert Dave Maasland. "Vroeger dachten we altijd dat dit soort hacks alleen in films gebeurden, maar we worden als samenleving steeds vaker met de neus op de feiten gedrukt dat het hacken van onze infrastructuur daadwerkelijk de realiteit is."

De oplossing is het vervangen van alle kwetsbare verkeerslichten. Daar zijn de wegbeheerders mee bezig. De verwachting is dat in 2030 de kwetsbare verkeerslichten zijn vervangen door nieuwe systemen.

Door IBD op 23 oktober 2024

Delen  

Blog: Hackbare stoplichten? CISO, grijp die kans!

Het recente onderzoek naar de kwetsbaarheid van verkeerslichten ([Tienduizenden verkeerslichten in Nederland te hacken, lek nog jaren te misbruiken, RTL Nieuws, 5 oktober 2024](#)) heeft veel stof doen opwaaien. Hoewel we dergelijke bevindingen als IBD altijd serieus nemen, blijft het belangrijk om zoiets in perspectief te plaatsen en nuchter te beoordelen. En misschien zelfs te benutten als CISO.

Pas op voor overhaaste conclusies

Het technische karakter van dit onderwerp maakt het voor bestuurders en managers lastig om een helder beeld te vormen van de daadwerkelijke risico's. Zeker als het gaat om de afwezigheid van een helder beeld. Het kan roepen als: "Dit is een ernstige hackbare stoplichten. Dit kan leiden tot overhaaste conclusies."

Wat is er aan de hand en hoe ernstig is het?


Op het eerste oog klinkt het alleen maar onacceptabel. Het zou onacceptabel zijn als tien stoplichten tegelijkertijd. Het feit dat de mogelijkheid bestaat, kan best acceptabel zijn. Het klinkt gek, maar veel van de genoemde 'ernstige risico's van dit zeer gevaarlijke lek' zijn vergelijkbaar met alledaagse(re) mogelijkheden die we wel gewoon (impliciet) accepteren. Een kwaadwillende zou bijvoorbeeld met een kilo spijkers uit de bouwmarkt (€ 9,35 met de voordeelpas) of een sloophamer (€ 42,95) vergelijkbare verstoringen op kruispunten kunnen veroorzaken. Maar dat gebeurt gelukkig niet, of niet zo vaak.

De enige oplossing?

Mijn oog viel op deze zin: "De enige oplossing is de verkeerslichten compleet vervangen, bevestigt het ministerie van Infrastructuur en Waterstaat (I&W)." Oplossing voor wat? De mogelijkheid dat een hacker dit kan? Bij het beoordelen van zulke radicale beveiligingsmaatregelen (vervangen van stoplichten) moeten we kijken naar zowel effectiviteit als


tegelijkertijd. Het feit dat de mogelijkheid bestaat, kan best acceptabel zijn. Het klinkt gek, maar veel van de genoemde 'ernstige risico's van dit zeer gevaarlijke lek' zijn vergelijkbaar met alledaagse(re) mogelijkheden die we wel gewoon (impliciet) accepteren. Een kwaadwillende zou bijvoorbeeld met een kilo spijkers uit de bouwmarkt (€ 9,35 met de voordeelpas) of een sloophamer (€ 42,95) vergelijkbare verstoringen op kruispunten kunnen veroorzaken. Maar dat gebeurt gelukkig niet, of niet zo vaak.

risico's van centralisatie




overbelasting IT-
security functie

①



IT security is niet goed in
proportionele risico-
inschattingen buiten het eigen
domein

②



kaders belemmeren
broodnodige risico-acceptatie
voor innovatie en veerkracht in
maatschappelijke opgaven

③

bovendien...

is IT dan wel goed in
security?



INFORMATIE
BEVEILIGINGS
DIENST

The Unpatchables: Why Municipalities Persist in Running Vulnerable Hosts

Aksel Ethembabaoglu, Rolf van Wegberg, Yury Zhauniarovich, and Michel van Eeten

Delft University of Technology

Abstract

Many organizations continue to expose vulnerable systems for which patches exist, opening themselves up for cyberattacks. Local governments are found to be especially affected by this problem. Why are these systems not patched? Prior work relied on vulnerability scanning to observe unpatched systems, notification studies on remediating them, and on user studies of sysadmins to describe self-reported patching behavior, but they are rarely used together as we do in this study. We analyze scan data following standard industry practices and detect unpatched hosts across the set of 322 Dutch municipalities. Our first question is: Are these detections false positives? We engage with 29 security professionals working for 54 municipalities to collect ground truth.

All detections were accurate. Our approach also uncovers a major misalignment between systems that the responsible CERT attributes to the municipalities and the systems the practitioners at municipalities believe they are responsible for. We then interviewed the professionals as to why these vulnerable systems were still exposed. We identify four explanations for non-patching: *unaware, unable, retired and shut down*. The institutional framework to mitigate cyber threats assumes that vulnerable systems are first correctly identified, then correctly attributed and notified, and finally correctly mitigated. Our findings illustrate that the first assumption is correct, the second one is not and the third one is more complicated in practice. We end with reflections on how to better remediate vulnerable hosts.

Dutch Safety Board investigated the incidents following the 2020 Citrix vulnerabilities and concluded that municipalities struggle with patching because of a lack of resources [17].

The threat of exploitation of local governments, or any other organization, is not hypothetical. Municipalities worldwide have been hit with ransomware attacks paralyzing organizations and losing sensitive and personal information of citizens [10, 24, 43, 45]. These attacks had destabilizing societal effects, with governmental services being unavailable and data of citizens being lost. In the US alone, more than a hundred local government organizations reported cyberattacks in 2019 and 2020 [42].

To mitigate such threats, governments established Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) [19]. These organizations receive security incident data and network scan information from various sources. This data is forwarded to the organization responsible for the vulnerable systems. The notified organization is then expected to mitigate the vulnerability. Prior research shows that such security notifications can expedite vulnerability remediation [32, 52]. CERTs around the world operate on a similar model of monitoring networks and notifying constituents. In Brazil, the CERT provides incident analysis and coordination services for any network that uses IP addresses or Autonomous Systems allocated to Brazil, and domains under the .br ccTLD. It alerts Brazilian networks involved in malicious activities [8]. The CERT-Bund in Germany supports handling IT security incidents; it provides active alerts for the federal administration in the event of acute threats [21]. In Africa, the non-profit organization AfricaC-

Ongepatchte systemen

- Samenwerking met IBD
- Netwerk-scans uitgevoerd
- Met lijsten van kwetsbare systemen naar IT-beheerders van gemeenten
- Vraag: waarom zijn deze systemen niet gepatcht?

(Rapport: "The Unpatchables"
USENIX 2024)



INFORMATIE
BEVEILIGINGS
DIENST

Ongepatchte systemen

- Antwoord IT-beheerder: “Dit systeem ken ik niet / is niet van ons”
- Oftewel: het systeem valt onder de verantwoordelijkheid van de gemeente, maar *niet* van IT-afdeling
- Zwart gat in beheer, waarin ook kwetsbaarheidsmeldingen voor OT verdwijnen

The Unpatchables: Why Municipalities Persist in Running Vulnerable Hosts

Aksel Ethembabaoglu, Rolf van Wegberg, Yury Zhauniarovich, and Michel van Eeten

Delft University of Technology

Abstract

Many organizations continue to expose vulnerable systems for which patches exist, opening themselves up for cyberattacks. Local governments are found to be especially affected by this problem. Why are these systems not patched? Prior work relied on vulnerability scanning to observe unpatched systems, notification studies on remediating them, and on user studies of sysadmins to describe self-reported patching behavior, but they are rarely used together as we do in this study. We analyze scan data following standard industry practices and detect unpatched hosts across the set of 322 Dutch municipalities. Our first question is: Are these detections false positives? We engage with 29 security professionals working for 54 municipalities to collect ground truth.

All detections were accurate. Our approach also uncovers a major misalignment between systems that the responsible CERT attributes to the municipalities and the systems the practitioners at municipalities believe they are responsible for. We then interviewed the professionals as to why these vulnerable systems were still exposed. We identify four explanations for non-patching: *unaware, unable, retired and shut down*. The institutional framework to mitigate cyber threats assumes that vulnerable systems are first correctly identified, then correctly attributed and notified, and finally correctly mitigated. Our findings illustrate that the first assumption is correct, the second one is not and the third one is more complicated in practice. We end with reflections on how to better remediate vulnerable hosts.

Dutch Safety Board investigated the incidents following the 2020 Citrix vulnerabilities and concluded that municipalities struggle with patching because of a lack of resources [17].

The threat of exploitation of local governments, or any other organization, is not hypothetical. Municipalities worldwide have been hit with ransomware attacks paralyzing organizations and losing sensitive and personal information of citizens [10, 24, 43, 45]. These attacks had destabilizing societal effects, with governmental services being unavailable and data of citizens being lost. In the US alone, more than a hundred local government organizations reported cyberattacks in 2019 and 2020 [42].

To mitigate such threats, governments established Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) [19]. These organizations receive security incident data and network scan information from various sources. This data is forwarded to the organization responsible for the vulnerable systems. The notified organization is then expected to mitigate the vulnerability. Prior research shows that such security notifications can expedite vulnerability remediation [32, 52]. CERTs around the world operate on a similar model of monitoring networks and notifying constituents. In Brazil, the CERT provides incident analysis and coordination services for any network that uses IP addresses or Autonomous Systems allocated to Brazil, and domains under the .br ccTLD. It alerts Brazilian networks involved in malicious activities [8]. The CERT-Bund in Germany supports handling IT security incidents; it provides active alerts for the federal administration in the event of acute threats [21]. In Africa, the non-profit organization AfricaC-

Windows Update

*Some settings are managed by your organisation

[View configured update policies](#)



You're not up to date

Last checked: Yesterday, 12:33

Your device is missing important security and quality fixes.

[Check for updates](#)



Patching in IT

- Gewone IT patching is ook allesbehalve “opgelost”
- Overheid en infrabeheerders verwerken maar een fractie van alle kwetsbaarheidsmeldingen
- Studie publieke organisatie: BIO deadline van 1 week voor “high high” advisories van NCSC wordt maar in 32% van de gevallen gehaald

Speedrunning the Maze: Meeting Regulatory Patching Deadlines in a Large Enterprise Environment

Gerbrand ten Napel
Delft University of Technology
G.H.TenNapel@tudelft.nl

Michel van Eeten
Delft University of Technology
M.J.G.vanEeten@tudelft.nl

Simon Parkin
Delft University of Technology
S.E.Parkin@tudelft.nl

Abstract—Many enterprises struggle to apply security patches in time to remove the risk of security breaches. Delays can be attributed to technical dependencies, outdated asset inventories, and issues of scale. Governments have started pursuing a strategy of mandating through regulation the patching of a highly selective set of severe vulnerabilities under very strict deadlines. We worked with a large organization to examine the patching timelines under these regulatory deadlines. We analyze patching ticket-system entries for 81 security advisories over seven years, covering 944 CVEs. We complement this with nine interviews with professionals involved in managing patches. We find that 40.2% of advisories required patching action, with a median completion time of 13.2 days; advisories that do not end in requiring a patch have a median of 1.4 days. Completing the patching process in 48 hours – a recommended industry best practice – is achieved in just 16.2% of the cases. For the deadline of one week, under the Dutch BIO regulation, patching is achieved in 32.4% of the cases, while the performance against the typical CISA KEV deadlines is a bit more hopeful: 56.8% is patched in two weeks and 62.2% in three weeks. We find that some variance in delays can be explained by coordination effort, as measured by the number of involved teams and people. Overall, the strategy of regulatory deadlines for a highly selective set of priority vulnerabilities is associated with much faster enterprise patching. The deadlines are routinely missed, yet they need to trade off realism versus exposure. The three-week KEV deadline is more feasible than the 48-hour one, yet it also leaves open a longer exposure window for exploitation.

quire organizations to take “appropriate” measures to handle vulnerabilities, and impose liability for when such measures are insufficient. Others go one step further, and impose mandatory patching deadlines for the most critical vulnerabilities.

The leading example of this strategy is the U.S. Cybersecurity and Infrastructure Security Agency (CISA)’s Binding Operational Directive 22-01 [8]. It legally requires federal agencies to remediate each vulnerability that is added to the CISA-managed Known Exploited Vulnerabilities (KEV) catalog within a specified deadline. Vulnerabilities listed in the catalog are prioritized as they are actively being exploited in the wild. Prioritization is a key part of this strategy: KEV contains a lot fewer vulnerabilities than those rated as critical under CVSS (Common Vulnerability Scoring System). The catalog currently contains just over 1,000 vulnerabilities – roughly 1% of all published vulnerabilities since 2021, when it was launched. The remediation deadline assigned to a new KEV addition is typically three weeks.

While the CISA directive is leading, it is not unique. In the Netherlands, where our study is located, there is a similar binding security policy for government organizations (called “BIO”) that requires agencies to patch within one week after receiving a top-priority advisory from the national CERT [9]. Like with KEV, the idea is to achieve much faster patching by radically prioritizing which vulnerabilities to focus efforts on. Regulations like BOD22-01 and BIO are not binding outside government, but they are a recommended best practice for private enterprises as well [10].

Does regulatory pressure lead to shorter patching timelines? Are the KEV or BIO deadlines achievable for en-

(Onderzoek: Speedrunning the Maze, IEEE S&P 2025; No One Drinks From the Firehose, IEEE S&P 2023)

Hoe ga ik om met kwetsbaarheden op IT systemen?

Vulnerability- en patchbeheer is het proces van het vinden en aanpakken kwetsbaarheden in de cybersecurity, betreffende elke asset met een connectie tot het TU Delft netwerk. Deze QRC geeft een toelichting voor een ieder die eigenaar is van een systeem binnen de TU Delft omgeving.

1 Scannen van de ICT middelen

De eigenaar van een systeem is verantwoordelijk voor het up-to-date en veilig houden van zijn of haar systeem. Om eventuele kwetsbaarheden inzichtelijk te krijgen, zal het systeem voorzien moeten worden van door ICT geleverde scantooling. .

2 Bepalen scoring kwetsbaarheid

Hieronder is de tabel met patching tijdslijnen weergegeven, gebaseerd op verschillende factoren. Voor meer info over [Dataclassificatie](#), [Vulnerability Management](#) of de [Baseline Informatiebeveiliging](#), klik op de bijgevoegde links.

3 Opgvolgingsproces

De eerste optie voor het verhelpen van een kwetsbaarheid is om deze te patchen. Aangezien het niet altijd mogelijk is om dit (tijdig) te doen, kunnen er andere stappen genomen worden in het opvolgingsproces:

Compenserende maatregelen

Indien patching op korte termijn niet mogelijk is, moeten compenserende maatregelen worden vastgesteld om het risico dat de TU Delft tijdens deze korte periode te beperken.

Incident management

Indien een vulnerability niet binnen de gestelde patch-tijdslijnen wordt verholpen, kan dit als beveiligingsincident beschouwd worden en daarmee via het SIRT het incident management proces doorlopen.

BIV classificatie	Ernst van de kwetsbaarheid	Risico score en asset waarde		
		Niet internet facing	Internet facing	In CISA database
		Patching tijdslijnen		
BIV-1	Kritisch	2 weken	1 week	2 weken
	Hoog	1 maand	2 weken	1 maand
	Middel	2 maanden	3 weken	2 maanden
BIV-2	Laag	Best effort	1 maand	Best effort
	Kritisch	2 weken	1 dag	1 week
	Hoog	1 maand	1 week	2 weken
BIV-3	Middel	2 maanden	2 weken	3 weken
	Laag	Best effort	1 maand	1 maand
	Kritisch	2 weken	1 dag	36 uur
BIV-3	Hoog	1 maand	48 uur	1 week
	Middel	2 maanden	1 week	2 weken
	Laag	Best effort	1 maand	1 maand

Uitzondering

Het kan zijn dat de kwetsbaarheid niet binnen de hersteltijdslijnen gepatcht of opgelost kan worden. Hiervoor kan de kwetsbaarheid (tijdelijk) worden geaccepteerd doormiddel van een risico acceptatie procedure.

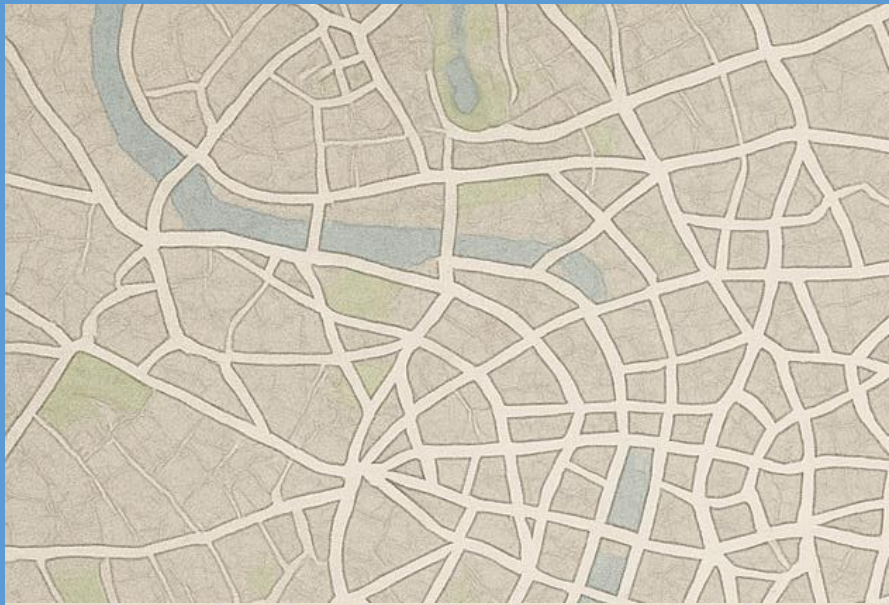
Patching in IT

- Interviews met 30 CISO's
- CISO ziet vaak niet of patchbeleid daadwerkelijk gehaald wordt
- Ziet patchbeleid als articulering van "ambitie", niet beschrijving van wat er echt gebeurt op de werkvloer
- Dit wordt niet beter met OT

wat dan wel?



- Wat als **wildgroei** en decentralisatie juist leiden tot meer **weerbaarheid**?
- Wildgroei is ook maatwerk, variëteit, veerkracht
- Laat verantwoordelijkheid liggen bij OT-beheerders
- En ondersteun hen, zonder een compliance keurslijf
- Samenwerking IT-OT



- Maar decentrale aanpak is 'onleesbaar' voor het bestuur
- "Wildgroei": niet te meten, te rapporteren, te sturen
- Dus organisatorische druk om te uniformeren, structureren, beheersen
- Uniformeren \neq beveiligen: weerbaarheid vraagt om vertrouwen in decentrale verantwoordelijkheid

Van wildgroei naar weerbaarheid

①

Niet iedereen mag z'n eigen feestje vieren

Decentrale verantwoordelijkheid \neq vrijblijvendheid. OT-beheerders maken vaak andere afwegingen – dat is legitiem, maar moet wél zichtbaar en bespreekbaar zijn.

"Weerbaarheid ontstaat pas als we de blinde vlekken durven blootleggen."

②

De CISO moet niet controleren – maar confronteren

De rol verandert: van regels handhaven naar ongemakkelijke vragen stellen. Wie monitort wat er aan het internet hangt? Wie controleert de claims van leveranciers?

"Pen-testing is geen compliance. Het is realiteitszin."

③

Uniformiteit maakt kwetsbaar

Wat beheersbaar oogt, is zelden echt veilig. De druk tot structureren en rapporteren leidt vaak tot schijnzekerheid. Diversiteit in systemen is lastig, maar ook robuust.

"De wildgroei is niet het probleem. De onzichtbaarheid is dat wel."