De cyber aanval op Oekraïene

## Inleiding

Doel van dit verslag is inzage te geven in de informatieverzameling en begrip van een complex scada systeem. De lezer krijgt inzage in de achtergrond achter cyberaanval, de gebruikte technieken en een opsomming van oplossingen en methoden voor beveiligingsvraagstukken.

## Algemeen

18 maart 2016 werd er een onderzoek gepublicerd van de E-ISAC. Een rapport met veel aanbevelingen waar ik in dit verslag alleen de aanbevelingen overneem voor een mitigatiestrategie.

<https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf>

analyse en mitigatiestrategie

<https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf>

In dit artikel wordt beweerd dat medewerkers op afstand konden inloggen op het SCADA netwerk en medewerkers op de netwerken voor Supervisory Control and Data Acquisitie hadden geen dubble- authorisatie nodig om in te loggen in het systeem.

<https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

<http://web.mit.edu/smadnick/www/wp/2016-22.pdf>

<https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack>

<https://www.wired.com/story/russian-hackers-attack-ukraine/>

<https://www.linkedin.com/notifications/>

<https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf>

<https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108>

<https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/>

<https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html>

Een overheidsinstantie van de Verenigde Staten biedt op haar website tekst en uitleg over een malware analyse van BlackEnergy malware.

<https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01>

Doel

Motivatie

## Opvallendheden

Na een analyse van bronnen die openbaar zijn gemaakt door instanties na onderzoek naar de stroomuitval bij energiebedrijven door media en onderzoekers is het duidelijk dat cyberaanvallen de oorzaak waren voor de stroomuitval in Oekraien. Het SANS ICS team heeft discussies gevolgd die gevoerd zijn door verschillende partijenen en organisaties in de internationale gemeenschap. Met enige zekerheid kan worden vastgesteld dat op basis van bedrijfsverklaringen, media rapportages, en eerstehand analyses he incident is veroorzaakt door een internationaal gecoordineerde aanval.

De aavallers tonen hierbij aan door planning, coordinatie, in combinatie met het gebruik van malware en de directe toegang op afstand de systeemcoordinators kunnen omzeilen. En erin slaagden de distributie van het elektriciteitsnetwerk te manipuleren en de resteloperaties voor de SCADA servers te vertragen nadat de schade op trad. De aanval bestond uit drie componenten: de malware, een Dos-aanval en een nog onbekend sluitend bewijststuk waarmee de impact werd geinitieerd. Huidige bewijsvoering suggerreert dat het missende component een directe interactie was van de aanvaller en niet het werk van malware.

De aanval werd bewerkstelligd door verschillende elementen waaronder de beperkingen voor ysteemcoordinators en het asluiten van telefoonlijnen om de ommunicatie naar buiten te saboteren. Met hoge zekerheid kan worden gesteld dat een coordinatie was waarbij meerdeere reginale energiecentra weden aangevallen.

Bij het uitvoeren van herstlwerkzaamheden werd er rekening gehouden met SCADA systemen die steeds geinfecteerd waren met malware. Medewerkers ter plaatse konden meedelen dat de substattions die werden aangevallen allemaal handmatig in plaats van automatisch werden herstart. De herstelwerkzaamheden duurden tussen de 3 en 6 werkuren.

Waarom is het aannemelijk dat malware wel is geactiveerd maar uiteindelijk niet de oorzaak was?

Er zijn twee theorien waarvan deeerste theorie beweert dat de KillDisk component aanwezig was in het netwerk maar niet de oorzaak was van de stroomuitval. De tweede theorie beweert dat de ‘KillDisk’ de directe oorzaak was voor het stroomuitval. Onderzoekers van SANS ICT beweren dat geen van beide theorien kloppen. Zij komen tot de conclusie dat malware de aanval mogelijk heeft gemaakt, de intentionele aanval, maar dat de KillDisk niet de oorzaak is geweest. De media gaat uit van BlackEnergy malware en het Sandworm team dat achter de aanval zou zitten. Maar het kan niet met zekerheid vastgesteld worden dat de excel bestanden die zijn aangetroffen bij de aanval samen met andere malware betrokken waren bij dit incident. Onderzoekers van SANS gaan er vanuit dat de malware bedoelt was om informatie uit bestanden te verzamelen di het mogelijk maken om de SCADA systemen niet te egbruiken of het gebruik daarvan te vertragen. Argument dat hiervoor is opgevoerd is dat de impact die is geconstateerd niet relateerd aan de schade van eerdere aanvallen waar dergelijke malware werdt gebruikt. Er wordt namelijk gesteld dat het draaien van een systeem zonder de voordelen die SCADA nou eenmaal biedt de risico’s op distributieniveau verhoogt maar zonder een status-wijziging kan er nog steeds stroom geleverd worden.

<https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/>

<https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm/u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108>

<https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN>

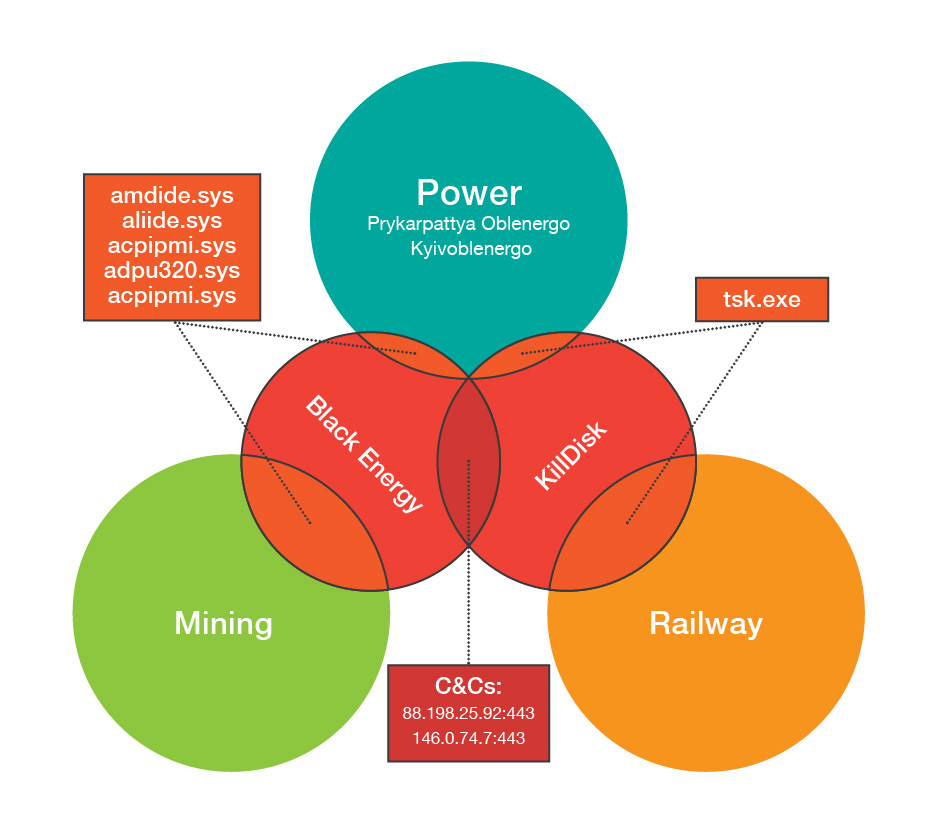
<https://www.wired.com/2014/10/russian-sandworm-hack-isight/>

<https://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/>

Dit artikel schets een situatie waarin er een overlap is van 5 samples van malware tussen de verschillende malware van het typpe BlackEnergy die is gebruikt bij de aanval op de krachtcentra en de mining-industrie in Oekraine.

In mindere mate is er een spilover van het gebruik van KillDisk bij de aanval op de mijn-sector en de aanval op de krachtcentralen.

Overal genomen is er een overlap bij het gebruik van malware als er gekeken wordt naar de naming-conventies, type malware, infrastructure en het tijdsslot waarin de malware werd gebruikt. Maar er wordt geen hard bewijsgeleverd wat de actieve rol was van de malware in de diverse fasen van de aanval.



<https://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/>

<https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf>

<https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/>

<https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802>

<https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf>

<https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf>

Speculaties

Vermoedelijk cybercriminelen en staatsactoren

## BlackEnergy

Is een destructieve malware vermoedelijk ontwikkeld in Rusland en wijdverspreid in industriele systeemtechnologie. (ukraine-power-grid-attack-russia-us, 2016)

In December 2014, DHS concerned that a BlackEnergy 3 malware variant was present in a Ukraine energy system that was attacked, causing a power outage.

ICS-CERT published a special TLP Amber version of an alert containing additional information about the malware, plug-ins, and indicators to the DHS secure portal website.

ICS-CERT strongly encouraged asset owners and operators to use the indicators to look for

signs of compromise within their control system environments.

## Ukraine Power Grid

Wat dit onderzoek niet bevat is een theorie over de betrokkenheid van een organisatie bij het uitvoeren van een dergelijke aanval zoals omschreven in het volgende artikel. Reden hervoor is dat de identificatie van een organisatie of rechtspersoon bedoeld is om een verantwoordelijke te beschuldigen voor een cyberaanval. Uit openbare bronnen die niet direct gelukt zijn aan bijvoorbeeld de amerikaanse autoriteiten blijkt dat de organisatie Sandworm voor de aanval verantwoordelijk wordt gehouden sinds haar activiteiten in oktober 2014.

(rand.org, sd)

De cuberaanval wordt op de voeten gevolgd door de amerikaanse inlichtingendiensten en de FBI omdat amerikaanse industriele complexen dezelfde kwetsbaarheden tonen als de systemen die actief gebruikt zijn in Oekraine. Het is daarmee ook de eerste cyberaanval met als gevolg de beinvloeding van de burgerbevolking en een aanslag op relevante kritische bedrijven en sectoren. De destructieve malware is volgende onderzoekers van Trend Micro ook gevonden bij mijnwinningsbedrijven en spoorwegbedrijven in de Oekraine.

(ukraine-sees-russian-hand-in-cyber-attacks-on-power-grid-idUSKCN0VL18E, sd)

Example 1: Attack on the Ukraine distribution system operator in 2015 The electric power sector was forced to take a more aggressive approach to cybersecurity following the 2015 attack on the Ukrainian power grid, affecting 27 substations and approximately 225,000 end customers.

Target was the Ukrainian electricity distribution company Kyivoblenergo.

The attack can be classified as an advanced persistent threat (APT) and resulted in a disruption of service and blackout.

The attackers used targeted emails carrying weaponised visual basic for application (VBA) Microsoft Word and Excel attachments.

Opening the files by employees installed a specific remote access tool (RAT) / malware, BlackEnergy3, on the workstations.

From there the attackers got access privileges for at least 6 months until they fully deployed specially crafted malware to the SCADA and field system enabling them to affect multiple substations.

Finally, they were able to open a series of breakers of multiple substations, triggering the blackout. Seven 110 kV and twentythree 35 kV substations were disconnected.

This incident received global attention and helped spread public awareness to the vulnerabilities of electric power systems.

A subsequent attack in December 2016 further exasperated industry concerns, with the country’s power grid quickly becoming a test bed of sorts for cyberattacks

<https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf>

In 2015, two days before Christmas, a cyber-attack cut electricity to

nearly a quarter-million Ukrainians. This is the \_rst known successful cyber-attack on a power grid.

Reuters reported that a power company located in the western portion of the Ukraine suffered a power outage, which impacted a large area that included the regional capital of Ivano-Frankivsk [55].

Attackers shut off power at 30 substations and left 230,000 people without electricity for up to six hours.

SCADA equipment was rendered inoperable, and power restoration had to be completed manually|further delaying restoration efforts [56].

Investigators discovered that attackers had facilitated the outage by using the BlackEnergy malware to exploit the macros in Microsoft Excel documents.

The malware was planted onto the company's network using spear-phishing emails [57].

ICS-CERT and US-CERT worked with the Ukrainian CERT and international partners to analyze the malware and con\_rmed that a BlackEnergy 3 variant was present in the Ukrainian power system [52].

The Ukrainian intelligence community blamed the attack on Russian attackers [58].

BlackEnergy has been publically identified by DHS and the FBI to be part of the RIS GRIZZLEY STEPPE

[59] group.

At the request of the Ukrainian government, a U.S. interagency team comprised of representatives from ICS-CERT and US-CERT, as well as DOE, the FBI, and the North American Electric Reliability Corporation, traveled to the Ukraine to gather information about the incident and identify potential mitigations [33].

This attack taught the world that it is indeed possible to damage the power grid through a cyber-attack, and was a wake-up call to ensure that the U.S. power grid is forti\_ed against such attacks.

In the case of the Ukraine, the attackers used technically unsophisticated techniques to achieve their goal.

The Ukraine power grid attack was a signi\_cant event in cyber-history.

Opportunities Multiple opportunities existed for the adversary to execute its attack.

External to the oblenergos and prior to the attack, there was a variety of open‐source information available; including a detailed list of types of infrastructure such as Remote Terminal Unit (RTU) vendors and versions posted online by ICS vendors.

19 The VPNs into the ICS from the business network appear to lack two‐factor authentication.

Additionally, the firewall allowed the adversary to remote admin out of the environment by utilizing a remote access capability native to the systems.

In addition, based on media reporting, there did not appear to be any resident capability to continually monitor the ICS network and search for abnormalities and threats through active defense measures; like network security monitoring.

These vulnerabilities would have provided the adversary the opportunity to persist within the environment for six months or more to conduct reconnaissance on the environment and subsequently execute the attack.

20 Based on the details provided in the DHS report, the adversary used a consistent attack approach on all three impacted targets.

The adversary also used consistent tactics to impact field controllable elements and irreparably damage field devices.

Why these oblenergos were targeted remains an open debate.

Based on the public reporting, it is unknown if the targets were selected based on common technologies in use, system architectures, reconnaissance operations, or service territories.

Opportunity‐based considerations for selecting a specific target may focus on an attacker’s confidence and ability to cause an ICS effect.

Some example decision factors could include:

• Targets with common systems and configurations • Multiple systems with common centralized control points

• ICS impact duration estimates (e.g., long term orshort term)

• Existing capabilitiesrequired to achieve desired results

• Risk level of performing the operation and being discovered

• Achieved access and ability to move and act within the environment

## Second Attack on the Ukraine Power Grid

Ook de tweede aanval op oekrainse kritische infrastructuur wordt toegerekend aan Sanndstorm. De KillDisk software die hier wordt gevonden wordt vergelijken met de software die gevonden werdt bij de hack op de Ukraiense verkiezingen in oktober 2015. (2016 ) KillDisk software verwijidert bestanden op de schijf, in dit geval van de systeemoperators. Maar dat niet alleen. KillDisk verwijdert ook de master boot record. Zodoende konden de computers crashen maar niet rebooten.

On December 17, 2016, almost one year after Ukraine suffered a major cyber-attack on its power grid, Kiev suddenly went dark again.

Cyber-attackers caused monitoring stations to suddenly go blind.

Break-ers tripped in 30 substations, turning o\_ electricity to approximately 225,000 customers.

To prolong the outage, attackers also launched a telephone denial-of-service attack (TDoS) against the utility's call center to prevent customers from reporting the outage, the same tactic that was used in 2015.

The intruders also rendered devices, such as serial-to-Ethernet convertors, inoperable and unrecoverable on their way out to make it harder to restore electricity to customers [64].

Despite these setbacks in the original attack, power was restored in three hours in most

cases, but because the attackers had sabotaged management systems, workers had to travel to substations and manually close breakers the attackers had remotely opened [56], [57].

However, the second attack was much more sophisticated than the first [64].

Where the first attack used remote control software to manually trip breakers, the second is believed to have used sophisticated malware that directly manipulated SCADA systems.

Rob Lee with Dragos Security said, In my analysis, nothing about this attack looks like it's singular.

The way it's built and designed and run makes it look like it was meant to be used multiple times. And not just in Ukraine" [65].

The sophisticated malware used in that second attack would later be identi\_ed as

CRASHOVERRIDE."

Dragos Security, working in coordination with the Slovak anti-virus \_rm ESET, confirmed that the CRASHOVERRIDE (or \Industroyer") malware was indeed employed in the December 17, 2016, cyber-attack on a Kiev, Ukraine transmission substation, which resulted in the large power outage [65], [66].

According to Dragos, CRASHOVERRIDE was the first ever malware framework specifically designed and deployed to attack electric grids.

It is the fourth-ever piece of ICS-tailored malware used against specific targets, with Stuxnet, BlackEnergy-2, and Havex being the first three.

It is the second malware ever designed and deployed for disrupting physical industrial processes, with Stuxnet being the first [65].

Dragos also stated that the functionality in the CRASHOVERRIDE framework serves no

espionage purpose, and the only real feature of the malware is for attacks leading to electric outages.

The CRASHOVERRIDE malware is a framework that has modules specific to ICS protocol stacks, including IEC 101, IEC 104, IEC 61850, and OPC.

It is designed to allow the inclusion of additional payloads

like DNP3, but at the time, no such payloads had been confirmed.

The malware also contained additional non-ICS specific modules, such as awiper, to delete \_les and disable processes on the running system for a destructive attack to operations [65].

The modules in CRASHOVERRIDE are leveraged to open circuit

breakers on remote terminal units (RTUs) and force them into an infinite loop to keep the circuit breakers open, even if grid operators attempted to close them, which resulted in the de-energization of substations forcing grid operators to switch to manual operations in order to restart power

[65].

Dragos says there are concerns CRASHOVERRIDE could be lever-

aged to disrupt grid operations that would result in power outages lasting

hours.

They assess that power outages could last up to a few days if an attack targeted multiple sites.

However, Dragos also pointed out that there is no evidence that threat actors could use CRASHOVERRIDE to cause any power outages to last longer than that.

But to even get a few days of power outages would require the targeting of multiple sites

simultaneously, which is entirely possible, but not trivial [65].

Using the National Cyber Awareness System (NCAS), DHS issued a CRASHOVERRIDE malware Technical Analysis alert on June 12, 2017, notifying U.S. critical infrastructure of the serious threat the malware poses [67].

The significant takeaway from the discovery of CRASHOVERRIDE is that nation state threat actors have created an advanced reusable malware framework specifically designed to cause power outages.

This same threat actor has demonstrated on multiple occasions that it is willing and able to cause power outages through cyber-means.

## De fouten van de verschillende protollen die gebruikt werden bij de SCADA systemen.

IEC\_60870-5

<http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0513EED48102FDAD1BD940260EF12B11?doi=10.1.1.548.7490&rep=rep1&type=pdf>

<https://scialert.net/fulltext/?doi=tasr.2014.396.405>

<https://www.researchgate.net/publication/333671061_Attacking_IEC-60870-5-104_SCADA_Systems>

<http://www.salvage-project.com/uploads/4/9/5/5/49558369/art3_-_salvage_2015_-_cyber_security_in_communication_of_scada_systems_using_iec_61850.pdf>

<https://eg.uc.pt/bitstream/10316/35720/1/Security%20Probes%20for%20Industrial%20Control%20Networks.pdf>

<https://owlcyberdefense.com/products/data-diode-products/software-modules/iec-104/>

<https://ris.utwente.nl/ws/files/6028066/3-s2_0-B9780128015957000227.pdf>

<https://waterfall-security.com/static/Waterfall-for-IEC-60870-5-104_FINAL.pdf>

<http://www.scada.sl/2013/11/last-week-four-guys-of-scada.html>

<https://repositorio-aberto.up.pt/bitstream/10216/119066/2/315683.pdf>

<https://www.diva-portal.org/smash/get/diva2:1046339/FULLTEXT01.pdf>

<https://www.semanticscholar.org/paper/Cybersecurity-analysis-of-a-SCADA-system-under-and-Rocha/dfa7c12551ebe7b24da8d806e87e946051a57cb9>

<https://control.com/forums/threads/comparison-between-iec60870-5-103-and-modbus-rtu.20317/>

<https://www.blackhat.com/docs/us-17/wednesday/us-17-Staggs-Adventures-In-Attacking-Wind-Farm-Control-Networks.pdf>

<https://www.securonix.com/web/wp-content/uploads/2019/08/RSAC_2019_Scada_Attack_Detection_101.pdf>

<https://dreamlab.net/en/blog/post/fuzzing-ics-protocols/>

<https://library.e.abb.com/public/f74f9c8be95f4cd09b0b1fbbde699108/4CAE000416_RTU_Secure%20communications_web.pdf>

<https://www.slideshare.net/qqlan/scada-zn>

<https://virsec.com/virsec-hack-analysis-deep-dive-into-industroyer-aka-crash-override/>

<https://tutcris.tut.fi/portal/files/16294332/jafary_1534.pdf>

<http://www.connectivity4ir.co.uk/article/175490/IEC-62351--Secure-communication-in-the-energy-industry.aspx>

<https://www.win.tue.nl/~setalle/2017_fauri_encryption.pdf>

<https://assets.barracuda.com/assets/docs/dms/Barracuda_CloudGen_Firewall_SB_Security_for_ICS_and_OT.pdf>

<https://www.checkpoint.com/products/industrial-control-systems-appliances/>

<https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>

<https://dl.acm.org/doi/fullHtml/10.1145/3381038>

<https://arxiv.org/pdf/2001.02925.pdf>

### <http://blog.nettedautomation.com/2017/>

IEC 61850, hack

iec 104

opc

iec 101

## CRASHOVERRIDE

<https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf>

## Manier om de aanvaller te ondermijnen

1. Management
   1. Company security policies in place
   2. Security policies written and enforced through training
   3. Computer software and hardware asset list
   4. Data classified by usage and sensitivity
   5. Established chain of data ownership
2. Employees
   1. Training on phishing, handling suspicious emails, social engineering hackers
   2. Password training and enforcement
   3. Training on dealing with strangers in the workplace
   4. Training on carrying data on laptops and other devices and ensuring the security of this data
   5. All security awareness training passed and signed off ensuring that all employees not only understand the importance of security but are active guardians for security
   6. Ensure that Secure Bring Your Own Device (BYOD) plans are in place
3. Business practices
   1. Emergency and cybersecurity response plans
   2. Determine all possible sources of business disruption cybersecurity risk
   3. Plans in place to lessen business disruptions and security breaches
   4. Emergency disaster recovery plans in place
   5. Alternative locations for running business in case of emergencies or disruptions
   6. Redundancy and restoration paths for all critical business operations
   7. Have you tested your restoration and redundancy plans?
4. IT staff
   1. System hardening plans
   2. Automated system hardening on all operating systems on servers, routers, workstations, and gateways
   3. Software patch management automated
   4. Security mailing lists?
   5. Regular [security audits](https://reciprocitylabs.com/cloud-security-vs-traditional-security/) and penetration testing
   6. Anti-virus software installed on all devices with auto-updates
   7. Systematic review of log files and backup logs to make sure there are no errors
   8. Remote plans in place, as well as policies regarding remote access
5. Physical security
   1. Lock servers and network equipment
   2. Have a secure and remote backup solution
   3. Make sure keys for the network are in a secure location
   4. Keep computers visible
   5. Use locks on computer cases
   6. Perform regular inspections
   7. Prevent unauthorized users from entering the server room or even in the workstation areas
   8. Security camera monitoring system
   9. Keycard system required for secure areas
   10. Secure Data Policy in place and ensure users understand the policy through training
   11. Secure trash dumpsters and paper shredders to prevent dumpster diving
6. Secure data
   1. Encryption enabled wherever required
   2. Secure laptops, mobile devices, and storage devices
   3. Enable automatic wiping of lost or stolen devices
   4. Secure Sockets Layer (SSL) in place when using the Internet to ensure secure data transfers
   5. Secure email gateways ensuring data is emailed securely
7. Active monitoring and testing
   1. Regular monitoring of all aspects of security
   2. Regularly scheduled security testing
   3. External penetration testing to ensure your staff hasn’t missed something
   4. Scanning for data types to make sure they are secure and properly stored

<https://www.us-cert.gov/ics/Recommended-Practices>

## Bijlage A: Checklists

• Introduction to Network Security Audit Checklist:

• 2Record the audit details

• 3Make sure all procedures are well documented

• 4Review the procedure management system

• 5Assess training logs and processes

• 6Review security patches for software used on the network

• 7Check the penetration testing process and policy

• 8Test software which deals with sensitive information

• 9Look for holes in the firewall or intrusion prevention systems

• 10Make sure sensitive data is stored separately

• 11Encrypt company laptop hard disks

• 12Check wireless networks are secured

• 13Scan for unauthorized access points

• 14Review the process for monitoring event logs

• 15Compile your report

• 16Approval:

• 17Send your report to the relevant stakeholders

iso standaarden

<https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/04/201902-Handreiking-Information-Security-Management-System-ISMS-v2.0.pdf>

<https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/NL/Checklist_of_ISO_27001_Mandatory_Documentation_NL.pdf>

<https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/NL/Checklist_of_ISO_27001_Mandatory_Documentation_NL.pdf>

<https://www.iso.org/isoiec-27001-information-security.html>

<https://www.iso27001security.com/html/faq.html>

<https://www.iso27001security.com/ISO27k_FAQ.pdf>

<https://www.iso27001security.com/ISO27k_GDPR_mapping_release_1.pdf>

<https://webstore.iec.ch/preview/info_isoiec27019%7Bed1.0%7Den.pdf>

[https://web.archive.org/web/20150924001524/http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002003738](https://web.archive.org/web/20150924001524/http:/www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002003738)

<https://webstore.iec.ch/publication/25948>

<https://webstore.iec.ch/publication/6912>

<https://webstore.iec.ch/publication/6911>

<https://www.ipcomm.de/protocol/IEC62351/en/sheet.html>

UK NCSC Guidelines

BDEW and Oesterreichs Energie

NERC CIP

<https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0>

<https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1>

<https://nvlpubs.nist.gov/nistpubs/ir/2010/NIST.IR.7628.pdf>

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

<https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf>

# Bibliografie

(n.d.). Retrieved from rand.org: https://www.rand.org/pubs/research\_reports/RR2081.html

(n.d.). Retrieved from dpstele.com: https://dpstele.com/blog%20major%20scada%20hacks

*/checklist/network-security-audit-checklist/#related-checklists*. (n.d.). Retrieved from process.st: https://www.process.st/checklist/network-security-audit-checklist/#related-checklists

(2016 ). Retrieved from https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html

*cybersecurity-audit-checklist*. (n.d.). Retrieved from reciprocitylabs.com: https://reciprocitylabs.com/cybersecurity-audit-checklist/

*ukraine-power-grid-attack-russia-us*. (2016, 2 11). Retrieved from edition.cnn.com: https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html

*ukraine-sees-russian-hand-in-cyber-attacks-on-power-grid-idUSKCN0VL18E*. (n.d.). Retrieved from reuters.com: https://www.reuters.com/article/us-ukraine-cybersecurity/ukraine-sees-russian-hand-in-cyber-attacks-on-power-grid-idUSKCN0VL18E