GOED BESTUUR &TOEZICHT
PLATFORM VOOR GOVERNANCE

Hoe maak je je organisatie weerbaar

Introductie

Incidenten met gijzelsoftware en datalekken laten zien dat cybersecurity een cruciaal aandachtspunt is. Met de toenemende afhankelijkheid van de digitale infrastructuur worden ook de dreigingen groter. Cyberaanvallen raken het functioneren van organisaties in het hart. De continuïteit van de primaire processen is dan in het geding. Wolter Pieters licht de noodzaak van een gedegen risicomanagement toe. Hoe moet de organisatie worden ingericht, zodat risico's die met cybersecurity te maken hebben zo goed mogelijk het hoofd kunnen worden geboden? En welke vragen moet de toezichthouder ter sprake brengen over cyberveiligheid?

Titel	:	Hoe maak je je organisatie weerbaar
Auteur	:	
Verschenen in	:	Goed Bestuur & Toezicht (Goed Bestuur & Toezicht 3/2021)
Publicatiedatum	:	18-09-2021
Tags	:	cybersecurityweerbaarheid

Incidenten met gijzelsoftware en datalekken laten zien dat cybersecurity een cruciaal aandachtspunt is. Met de toenemende afhankelijkheid van de digitale infrastructuur worden ook de dreigingen groter.
Cyberaanvallen raken het functioneren van organisaties in het hart. De continuïteit van de primaire processen is dan in het geding.

Wolter Pieters licht de noodzaak van een gedegen risicomanagement toe. Hoe moet de organisatie worden ingericht, zodat risico's die met cybersecurity te maken hebben zo goed mogelijk het hoofd kunnen worden geboden? En welke vragen moet de toezichthouder ter sprake brengen over cyberveiligheid?

Wolter Pieters is hoogleraar Work, Organisations and Digital Technology aan de Radboud Universiteit. Zijn onderzoek richt zich op de effecten van digitale technologie en veilig gedrag in organisaties.

HOE MAAK JE JE ORGANISATIE WEERBAAR?

VIERLUIK
1

Eerder dit jaar was het groot in het nieuws: een datalek bij de GGD's, waardoor persoonsgegevens van mensen die een coronatest hadden aangevraagd konden worden verhandeld.[1] Oorzaak: een functie voor grootschalige download van gegevens was voor alle medewerkers beschikbaar. En daar werd misbruik van gemaakt. Daarnaast werd ook niet systematisch bijgehouden wie die functionaliteit gebruikte.
Ook ging het dit jaar weer bij verschillende organisaties mis met ransomware (gijzelsoftware), onder andere bij de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en bij een meubelconcern. Dit terwijl de Universiteit Maastricht al meer dan een jaar geleden uitgebreid informatie deelde over hoe het bij hen fout had kunnen lopen. Het symposium van de Universiteit Maastricht begon met het tonen van 'patiënt zero': de laptop waarop een link in een phishing e-mail werd geopend. Daarmee begon een serieuze cybercrisis. Rond de jaarwisseling van 2019-2020 werd een groot deel van netwerk en data vergrendeld. De universiteit betaalde uiteindelijk twee ton losgeld aan de cybercriminelen om de primaire processen weer op gang te krijgen.

Deze aanval is zeker niet uniek. Wat wel uniek is, is de openheid waarmee over het incident werd gecommuniceerd.[2] De analyse geeft een goed beeld van hoe zo'n cyberaanval in zijn werk gaat. Eerst bemachtigen de aanvallers via phishing een of meerdere accounts van medewerkers. Vervolgens wordt gekeken of er mogelijkheden zijn om verder in het netwerk door te dringen, bijvoorbeeld via verouderde software en/of ontbrekende afscherming. Als de aanval dan niet wordt opgemerkt door monitoring kunnen de aanvallers in feite hun gang gaan, tot ze het genoeg vinden en de gijzelsoftware uitrollen op die delen waar ze controle over hebben.
Incidenten met gijzelsoftware en datalekken laten zien dat cybersecurity een cruciaal aandachtspunt is. Met de toenemende afhankelijkheid van digitale infrastructuur worden ook de dreigingen groter. Door het thuiswerken tijdens de coronacrisis is dat alleen maar duidelijker geworden. Daarbij heeft gijzelsoftware het speelveld fundamenteel veranderd. Er zijn namelijk bij de Universiteit van Maastricht, in tegenstelling tot bij de GGD's, helemaal geen data gestolen. Eerder kon je als organisatie nog denken: bij ons is niet veel gevoeligs te

halen. Maar het gaat nu niet meer alleen over de waarde van de data voor de aanvallers; het gaat over de waarde voor de organisatie zelf. Als criminelen de data kunnen blokkeren, dan kunnen ze losgeld vragen gebaseerd op wat de data voor jou waard zijn.

Risicomanagement

De toenemende dreiging spreekt ook uit het Cybersecurity Beeld Nederland dat onlangs gepubliceerd werd.[3] Zowel spionage als gijzelsoftware worden daarbij genoemd. Er wordt daarbij benadrukt dat cyberaanvallen het functioneren van organisaties in het hart raken, vanwege de afhankelijkheid van de digitale technologie. De continuïteit van de primaire processen is in het geding. Weerbaarheid is dus nodig, maar basismaatregelen zoals het updaten van software en het maken van backups zijn lang niet overal op orde.
De lessen die werden getrokken door de Universiteit van Maastricht kunnen ook richting geven aan cyberveiligheid in andere organisaties. Wat kun je dan als organisatie doen? De verleiding is groot om te denken dat het probleem met een firewall en een bewustwordingscampagne is opgelost. En dat de oplossingen dus gerust aan de IT- en HR-afdelingen kunnen worden overgelaten. Maar dat miskent dat we hier uiteindelijk te maken hebben met een probleem van risicomanagement, dat ingebed moet worden in hoe de organisatie als geheel met risico's wil omgaan. Wat voor risico's is de organisatie bereid te nemen? En hoe moet de organisatie worden ingericht zodat risico's die met cybersecurity te maken hebben zo goed mogelijk het hoofd worden geboden? Dat wil zeggen: hoe krijgen we de werkelijke risico's onder het acceptabele niveau?
Bij de aanval op de Universiteit Maastricht wordt duidelijk dat risico's op verschillende niveaus moeten worden afgedekt. Als er toch iets misgaat wordt vaak naar de mens gewezen als zwakste schakel, of als bron van menselijke fouten waardoor de technische oplossingen uiteindelijk niet werken ('Je had niet op die phishing link moeten klikken'). Maar dat is dus te simpel gedacht. Het gaat immers nooit lukken om alle phishing-pogingen te voorkomen, zelfs niet met intensieve training. Er gaan dus accounts in handen van criminelen komen. Wat dan telt, is hoe het computernetwerk is ingericht, met voldoende afgeschermde delen, en hoe de monitoring van dat netwerk problemen tijdig kan signaleren. En als het dan toch misgaat, is er dan een plan voor crisismanagement, en zijn er bijvoorbeeld recente offline backups die teruggezet kunnen worden?
Uiteindelijk gaat het erom hoe een organisatie met data wil omgaan, en hoe dat past binnen een bredere visie op risico's. Een simpele manier om incidenten te voorkomen of verkleinen, is data die niet echt nodig zijn überhaupt niet op te slaan. En als data wel opgeslagen worden, daar een passend beveiligingsniveau aan te koppelen, en dan ook te zorgen dat de data niet weggesluisd worden, naar minder veilige omgevingen. Dat vereist *defense-in-depth*: meerdere lagen van beveiliging. Preventie, detectie en respons moeten op orde zijn. Maar ook inbedding van cyberrisico's in processen, zodat maatregelen continu geëvalueerd en bijgesteld kunnen worden.

Schaduw IT

Een cruciale vraag is hoe cybersecurity verenigd kan worden met de primaire doelen van de organisatie. Beveiliging heeft vrijwel altijd impact die verder gaat dan de kosten van de aan te schaffen en onderhouden spullen. Het is daarbij van belang dat organisaties zich realiseren dat medewerkers zich wat betreft cybersecurity vrijwel altijd geconfronteerd zien met conflicterende normen. Als iets via de veilige weg moet duurt het langer, en als er haast bij is ligt een shortcut voor de hand. Bijvoorbeeld het delen van gevoelige informatie via een kanaal dat daar niet voor bedoeld is: zogenaamde 'schaduw IT', die zich onttrekt aan de controle van de organisatie. Daarbij geven medewerkers op hun eigen manier vorm aan security, die in meer of mindere mate effectief kan zijn.[4] Aanvallers maken ook handig gebruik van de sociale norm om hulp te bieden, en kunnen zo zowel fysiek (deur openhouden) of digitaal (ingaan op hulpverzoek in e-mail of telefoongesprek) toegang krijgen tot een organisatie.
Normen rond de prioriteit van het primaire proces en sociaal gedrag verander je niet zomaar, voor zover je dat

‘Het opstellen van policies rond cybersecurity leidt lang niet altijd tot het gewenste gedrag, en het effect van awareness-initiatieven is beperkt’

al zou moeten willen. Het opstellen van policies rond cybersecurity leidt dan ook lang niet altijd tot het gewenste gedrag, en het effect van awareness-initiatieven is beperkt.[5] Maar ook op het niveau van implementatie gaat vaak het nodige mis. Zo zag ik mijzelf geconfronteerd met een verzekeraar die een leeg formulier via een beveiligde omgeving aanbood voor download, maar vervolgens vroeg om het ingevulde formulier met gevoelige data via de e-mail terug te sturen. Dat is dus niet de bedoeling. Als je een beveiligd platform inricht moet je het wel op de juiste manier gebruiken.
Er gaan dus zowel in implementatie als in gebruik regelmatig dingen mis. Daarbij kun je je afvragen of medewerkers begrijpen waarom maatregelen nodig zijn. Je kunt bijvoorbeeld wel VPN (een versleutelde verbinding met het bedrijf) aanbieden voor thuiswerkers, maar als de meerwaarde niet duidelijk is zal het gebruik beperkt blijven. Op dezelfde manier kun je een beveiligd platform voor het delen van bestanden implementeren, maar dan moeten medewerkers wel begrijpen waarom de bestanden niet gewoon per e-mail moeten worden verstuurd.
Leidinggevenden kunnen een belangrijke rol spelen, door op cruciale momenten uitleg te geven en door hun voorbeeldfunctie. Daarnaast kunnen ze laten zien dat ze signalen rond problemen serieus nemen, zodat medewerkers eerder geneigd zijn mogelijke zwakheden te melden. Zo wordt ook een organisatorisch klimaat gecreëerd waarin cyberveiligheid en privacy meer op de voorgrond komen te staan.[6]

Testen, testen, testen

De vele fouten die gemaakt worden laten ook zien dat organisaties op tijd experts moeten inschakelen om mee te kijken. Dat geldt voor het ontwerp en de configuratie van systemen, maar ook voor het systematisch testen op zwakheden in de bedrijfsfase.[7] Deze zogeheten *penetration tests* door ethische hackers geven vaak cruciale informatie voor het op tijd verhelpen van kwetsbaarheden. Het openzetten van een download-functie voor databases (zoals in het geval van het GGD-lek) of verouderde software (zoals vaak misbruikt bij gijzelsoftware) zou dan direct moeten opvallen. Soms wordt een organisatie ook spontaan door een ethische hacker gewezen op een kwetsbaarheid, de zogenaamde *responsible disclosure*.[8] Is het dan duidelijk wat daarmee gedaan wordt? Hoe wordt de melding onderzocht, opgevolgd, en afgerekend met de melder?
En als het dan toch misgaat, ligt er dan een plan voor crisismanagement? En is er met dat plan geoefend? Zijn er offline backups, en hoe moeten die teruggezet worden? Is er nagedacht over de mogelijkheid van een cyberverzekering? Is het duidelijk welke informatie er wanneer met wie gedeeld moet worden?[9]

Investeringen

Hoeveel zou een organisatie dan moeten investeren in cybersecurity? Dat is lastig te zeggen. Vanuit de juridische kaders, zoals de Algemene verordening gegevensbescherming (AVG) wordt gevraagd om passende technische en organisatorische maatregelen. Er moet dus vastgesteld worden wat voor de organisatie passend is. Daarnaast is er de interne afweging hoe groot de kans op incidenten met een bepaalde schadeomvang wordt geschat, en wat de organisatie bereid is aan risico te dragen. Er is weinig bewijs voor de mate waarin specifieke maatregelen in het algemeen effectief zijn.[10] Om iets te kunnen zeggen over de effectiviteit binnen de eigen organisatie zal in ieder geval ook bijgehouden moeten worden in welke mate incidenten

‘De Universiteit Maastricht betaalde twee ton losgeld aan cybercriminelen om de primaire processen weer op gang te krijgen’

voorkomen zijn door de maatregelen. Anders blijft de effectiviteit geheel onzichtbaar. (We zijn toch niet gehackt? Waarom hebben we dan al die maatregelen genomen?) Er is veel te bereiken door best practices te volgen, en de kosten daarvan zijn goed in te schatten, maar iedere organisatie zal ook een eigen afweging moeten maken over risico’s en bijbehorende maatregelen.

Cruciale vragen stellen

Er is in principe voldoende inzicht in hoe cyberaanvallers te werk gaan en hoe datalekken ontstaan, en wat een organisatie daartegen kan doen. Er is weliswaar weinig wetenschappelijk onderzoek naar de effectiviteit van maatregelen, maar veel (combinaties van) interventies hebben zich in de praktijk bewezen. Het is wel cruciaal dat organisaties de daarvoor benodigde kennis in huis halen. En zelfs als die kennis er is, niet blindvaren op een enkeling die verantwoordelijk is voor de implementatie, want het is te gemakkelijk om fouten te maken. En een kleine fout kan al grote gevolgen hebben.
De volgende vragen zijn cruciaal om te stellen als het gaat over cyberveiligheid in organisaties:

- Zijn beslissingen over cybersecurity-maatregelen gekoppeld aan een inschatting van de risico’s?
- Worden oplossingen op het gebied van detectie, preventie en respons voldoende getest?
- Begrijpen medewerkers waarom maatregelen worden genomen, en hoe zij door gedrag kunnen bijdragen aan de effectiviteit daarvan?
- Heeft de organisatie zicht op het gebruik van schaduw IT en de gevolgen daarvan voor de digitale veiligheid en privacy?
- Wordt er regelmatig geëvalueerd of de maatregelen effectief zijn en of er nieuwe interventies nodig zijn?

Met de afhankelijkheid van digitale technologie zijn de gevolgen van cyberaanvallen voor de hele organisatie merkbaar. Maar omgekeerd kan ook de hele organisatie bijdragen aan het vergroten van de digitale veiligheid.

Noten

1. https://www.security.nl/posting/706894/Z0%27n+1250+Nederlanders+slachtoffer+van+datadiefstal+bij+GGD.
2. https://www.maastrichtuniversity.nl/nl/updates-cyberaanval.
3. https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.
4. Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). ‘Shadow security’ as a tool for the learning organization. ACM SIGCAS Computers and Society, 45(1), 29-37.
5. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.
6. Timmermans, J. (2018). The relation between the organizational information security climate and employees’ information security behavior. Master’s thesis, TU Delft. https://repository.tudelft.nl/islandora/object/uuid%3A78a12359-a9a9-4b65-8e8f-83aeae8b8939?collection=education.
7. Pieters, W., Hadžiosmanović, D., & Dechesne, F. (2016). Security-by-experiment: Lessons from responsible deployment in cyberspace. *Science and engineering ethics*, 22(3), 831-850.
8. Kranenbarg, M. W., Holt, T. J., & van der Ham, J. (2018). Don’t shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime Science*, 7(1), 1-9.
9. Kulikova, O., Heil, R., van den Berg, J., & Pieters, W. (2012, december). Cyber Crisis Management: A decision-support framework for disclosing security incident information. In 2012 International conference on cyber security (pp. 103-112) IEEE.
10. Pieters, W. (2020). *Philosophy of Security Engineering. In The Routledge Handbook of the Philosophy of Engineering* (pp. 533-543). Routledge.