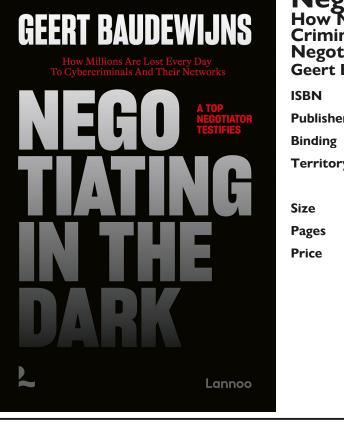


TITLE INFORMATION Tel: +44 (0) 1394 389950 Email: uksales@accartbooks.com Web: https://www.accartbooks.com/uk





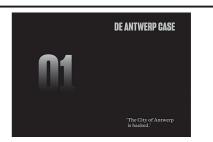
Negotiating In The Dark How Millions Are Lost Every Day To Cyber Criminals And Their Networks – A Top Negotiator Testifies Geert Baudewijns

ISBN	9789020919561
Publisher	Lannoo Publishers
Binding	Paperback / softback
Territory	World excluding Belgium, The Netherlands, France,
	Switzerland & Scandinavia
Size	210 mm x 140 mm
Pages	224 Pages
Price	£25.00
	223.00

- One of the world's top negotiators talks about his hunt for cybercriminals
- Cyberattacks threaten more and more companies, governments and citizens
- Geert Baudewijns, a Belgian cybersecurity expert, has negotiated for hundreds of hacking victims
- Page-turner with tips to protect ourselves

Geert Baudewijns, full-time ransomware negotiator, is called every week by hacked companies and governments across the globe. But by then, it's too late. Cybercriminals have infiltrated the system. To prevent worse-case scenarios – weeks of downtime, all your data leaked – over 70 percent of the victims give in to ransom demands. And malicious hacker collectives on the dark web are making fortunes. This is still a taboo because no one wants to go public with it. Who is at risk? How do hackers operate? How can we protect ourselves? In this book, Baudewijns takes the reader into the dark side of the digital world. His insider stories describe recent cases from around the world.

Geert Baudewijns is a cybercrime specialist and CEO of Secutec, an international cybersecurity company focused on providing tailored solutions to corporations, the financial sector, and government. He is one of the most sought-after cyber negotiators in the world.



Although my business card says something else, when people ask	as suppliers we were closely involved with Digipolis, the elig
what I do, I anually say: Negotiating with cyberoriesinals. That's	11 partner, responsible for an extension range of services, fre
the most clear-out supect of my work in cybersecurity: commu-	maintaining the city network to the digital development of o
nicating with backers who use ransomwate to pripple a compa-	services. Their remit also includes cybersecurity, something Ar
ny's network. Those hackers are always deviaing new ways to infitrate networks, install malicious software, encode all the	werp had taken particularly seriously since the Litige backing Litige was hit by a ransortware attack carried out is the Ro
data, and oncy it. Then they domand a ransom to revenue the en-	group in June 2025. A Belgian metropolis was brought to a star
errortion and not publish your data. Hackmail, pure and simple.	util for the first time. Media reports chain the city paid thirty n
The targeted companies have their backs to the wall. Nothing	Son in ranson, which art off alarm bells in Antworp, Orbersets
works anymory and they have no choice but to send their staff	ty way suddenly high up on the agenda and the city council ma-
home, suspend production and services, and have their rr per-	extra resources available to avoid a
sonnel clock up overtime. In most cases, they soon conclude that	spenario like the one in Lidge. With
paying the ransom is the quickest, most out-effective - or even	this is mind, they tasked Digipula, At the time of
the only - solution. That's when they come to me for help. As a	their technology partner, with development the backing, as
negotiator, my job incluto track down cybercriminals, but to talk	oping a comprehensive cybeneouri- suppliers, we
with them for days or even weeks. My goal is to drive down their	ty plan. The goal was clear, to relow were closely
prior and figure out how they got in. Of sourse, giving in to the	force the city's digital defences and involved with
domands of ansorupulous backers field galling, but I do all I can	make its systems cyberattack proof. Eligipolis, the
to minimise the ransom domand so that most companies survive	Digipolis put out several invitations city's rr partner.
an attack unscethed.	to tender, a few of which our compa-
	ny won. Specifically, our job was to
The most restorious backing in Flanders is probably the cyber-	track down and identify potential weak spots in the network. W
attack on the City of Artwarp in late 2023. Whenever I stylike	ware not involved in the operational side of things; our role w
up a conversation with someone and mention my work, I'm al-	to pispoint places where attackers could gain access. Our an
ways asked. What happened in Antworp? The cyberattack on	ysis uncovered numerous vulnerabilities, which instruncommo
the city, and on 5 December, 5t Nicholas' Eve of all nights, has	and something we see in many companies. Keep in mind that, II
sost none of its fascination, and is eached in the collective mem-	the networks of many other large cities, Antworp's infrastructu
cey. The story has all the ingredients to pique the imagination:	dates back at or 31 years.
an leonic date, a major city, and a mysterious desouement about	Many of our clients face the same issue. They start with
which rumours persist.	small network that needs to grow rapidly without disruption
For me, this is a loaded question because frankly, 'the Ant-	the operation of existing applications or services. Over the la
werp ease' still gets under my skin. At the time of the backing,	sypears, the digital transformation of eity services eaused th