Guaranteeing cybersecurity is never child's play, even for a large toy retailer

BY ANNA HAMMOND · FEBRUARY 28, 2023 · LAST UPDATED ON MARCH 6, 2025

2020 saw four years of eCommerce growth in a single quarter, according to Colliers, as nearly 150 million people shopped online for the first time. That's a staggering increase, and growth is predicted to continue at least through to the end of this decade.

This rapid growth means eCommerce infrastructure is expanding rapidly too, bringing new risks posed by increased attack surfaces, new technologies, and undiscovered vulnerabilities.

Established players who have previously undergone online expansion have much to teach us, and one such player is the children's toy retailer, Lobbes. Based in the Netherlands and operating since 1989, Lobbes maintains a cutting-edge web store that is as delightful as it is robust. And with a massive catalog of over 23,000 items available, they have the attention of millions of young eyes and their parents.

Lobbes considers cybersecurity a vital part of how they fulfill their mission. In everything from secure checkout to rapid fulfillment and customer information storage, Lobbes has made cybersecurity a business priority.

For such a large online presence, that's quite an undertaking! So today we're talking to Bert Brunekreeft, Head of ICT at Lobbes, to discuss how this retailer ensures cybersecurity in a world where cybercriminals are always at work.

Intigriti: Hi Bert! Thanks for taking the time to talk to us today! Lobbes is in the business of toys and play. Can you tell us a bit about your role as Head of ICT? Is it all fun and games too?

Bert: Well, fun is at the heart of what we do at Lobbes as a company, but we'd be no company at all without treating some things seriously! And ICT infrastructure management is definitely one of those things.

Given the scale and number of visitors to our web store, my team spends a lot of time ensuring that performance, maintenance, and development help fulfill Lobbes' strategic direction.

We don't just focus on the store, of course, though it is a high priority. Infrastructure needs are constantly evolving in all areas of our business, so we regularly assess then acquire and maintain new hardware and software resources and solutions. All of this has to fit in with best practices and, in many cases, legal standards. This can span anything from the customer-facing, such as GDPR data requirements, right through to what digital tools we use in the fulfillment warehouses. It's a lot to cover, but we do have to do it.

Moreover, the very important question of ongoing cybersecurity is always part of what we do. We don't treat security as an isolated activity. Efficiency and productivity, for example, are considered key to business success. We do the same for security.

Intigriti: Can you outline for us how you approach security for Lobbes?

Bert: Risk Management and cybersecurity are important aspects for all modern businesses. As I've said, they're not periphery issues but key elements in how you deliver on your company's mission. At Lobbes, a strong approach to risk management is especially important given the large number of our digital assets that are publicly facing. So we have to constantly be monitoring and improving our systems to make sure risk is under control. This includes backup and disaster prevention, as well as response and recovery procedures. Some of the work my team and I do is on internal systems and some for the public-facing assets.

ICT Teams need to implement security protocols, policies, and procedures to head off potential threats. Thankfully, we also have a lot of tools at our disposal these days to make our cybersecurity stronger: automated tools and vulnerability scanners, pentests, and, of course, bug bounty programs.

One thing is sure: if you are a business operating in the modern world, you are almost guaranteed to become a target of cybercriminals at one moment or another. That would be a very sad truth if there weren't things we can proactively do about the threats.

Intigriti: You just mentioned three different types of tools you use to protect your attack surface at Lobbes. Can you elaborate?

Bert: Sure. Cybersecurity and ICT as a whole are really like any other work: you'll get the best results if you use the right tool for the job.

Automated tools like vulnerability scanners, virus checks, password protocols, etc. play a really important role in ensuring basic good practices and security. Our staff are human, of course, and that means sometimes a person is going to make a mistake that is a security risk. Automated tools and procedures are a great way of making sure these slip-ups are controlled before they are exploited.

And then there is our wider attack surface. Not to put too fine a point on it, it is essential to absolutely hammer your defenses and see if they hold up. It's what a malicious hacker will do, after all, so you need to test precisely for the type of threats they pose.

We've found pentests useful because they are usually very comprehensive, but the problem is, most really skilled hackers are going to know what pentests test for too. They won't waste their time if they see your security is robust. They'll go looking for some new weakness instead: one that no one has thought of.

It's why we were excited to start a bug bounty program at Lobbes. Letting ethical hackers try to break through our security before someone malicious does seemed like a great idea to us.

Intigriti: How important is continuous testing at Lobbes?

Bert: First of all, I should say that continuous testing for Lobbes comprises two types of testing.

There are the tests my team and I are constantly running internally. We ask if all our security protocols are in place and are running effectively. We check all software is up-to-date and patched. There's a lot more and I listed some of these things in answer to your second question above.

The second type of ongoing security testing, using a bug bounty program, has become a new cornerstone of our IT security posture. I think almost any type of business can benefit from a bug bounty program. For Lobbes, with our large website plus order and supply chains, it feels like it has become really essential to maintaining good cybersecurity.

Intigriti: What benefits, in particular, have you seen with running a bug bounty program?

Bert: One thing really stands out: discovery of unknown threats.

At Lobbes, we have a really knowledgeable IT team. We patch everything fast, we use best practices, but the problem with cybersecurity threats is that they are constantly evolving as hackers make new discoveries. Even if we were aware of every known cybersecurity threat in the world today, there's a good chance that tomorrow a hacker somewhere is going to uncover a vulnerability that no one knows about.

Obviously with a large web presence like Lobbes', we are exposed to such attempts. The great thing about a bug bounty program is that it is ongoing and we know that the ethical hackers hitting our systems are just as inventive and motivated as any malicious hacker would be. So with this type of continuous testing, we have the best chance possible of finding vulnerabilities before a malicious hacker does. That is huge!

There are a lot of other advantages to using a good bug bounty platform, like Intigriti's, by the way. There's triage, support, easy setup, etc., but the number one reason we run a bug bounty program continuously is the one above.

Intigriti: Finally, do you have any tips for new businesses entering the online retail space?

Bert: Three tips. In regards to security, I have two.

First, the minute you start making untested assumptions is the minute the malicious hackers get ahead of you. It's part of your job these days to test everything and test constantly. Assume you will be attacked. Be ready and do your work!

The second security point is a wider business focus: treat security as fundamental to your business success. This is a slightly different way of thinking about security for most people. But it is a good way to get it ingrained in the mentality of your employees. Most employees will feel that things like "efficiency" and "productivity" and "creativity", etc. are natural and required parts of their work. I suggest adding "security" to that list and working to make sure it is embedded in your business culture. Going forward in our networked world, it is not an exaggeration to say it will be essential to your business mission.

And then there's one last tip, maybe the most important of all: when you're done with work, make sure you find some time to play too!

About Bert Brunekreeft

Bert Brunekreeft is the Head of ICT at Lobbes.nl, having joined the company in 2005. As a toy retailer, it is pivotal that Lobbes has a robust Cybersecurity strategy in place. Bert is responsible for leading and developing this important at Lobbes. He oversees all technology operations, and establishes IT policies and systems according to company needs. Before joining Lobbes, Bert worked at TriLogic and Automation as an Internet Consultant.