

WAF as a Unifying Technology for Development and Operations – an Interview with Daniel Stricharz of Telefónica O2 Germany

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Joining me today is Daniel Stricharz. Daniel is a senior security and infrastructure specialist at Telefónica O2 Germany. He is responsible for customer portals, and their value added services. Daniel has studied law and computer science. Before he joined the telecommunications arena in 2000, he worked as a consultant, both in the IT and legal arena, for international businesses.

His knowledge of emerging German legislation, cyber crime, and cyber law, gives him the ability to add value to complex technical and legal requirements. He initially specialized in data protection law and its technical implementation until he moved on to cover a full range of security aspects, from product development to the operations of online services.

Telefónica O2 Germany belongs to Telefónica Europe, and is part of the Spanish telecommunication group Telefónica S.A. The company offers its German private and business customers postpaid and prepaid mobile and telecom products as well as innovative mobile data services, based on the GPRS and UMTS technologies. In addition, the integrated communication provider also offers DSL, fixed network telephony, and high speed Internet. Telefónica Europe has nearly 47 million mobile and fixed network customers in Great Britain, Ireland, the Czech Republic, Slovakia, and Germany.

In Germany, where the customer is known simply as O2, with its headquarters located in Munich, Germany, they have a customer base of over 14.5 million. Besides its more than 750 shops, O2 operates a massive online portal, offering services ranging from an online shop over a complex web-based email solution, to a range of self service opportunities for customers in a huge number of other mobile services that help enrich the customer's mobile experience.

Welcome to the show, Daniel.

Daniel Stricharz: Hi Brian. It's a pleasure to be here.

Brian Contos: Daniel, perhaps you could give me a little bit of background about O2, what your business is, and a little bit more detail on your organization.

Daniel Stricharz: Sure, Brian. I'm working for Telefónica out of Germany, which is a mobile telecommunications provider in Germany. We offer superior UMTS technology to our customers, as well as DSL fixed networks telephony. And we are one of four mobile

operators in Germany. And we are located in Munich with our headquarters, but of course we have sites all over Germany. And Telefónica O2 Germany is the daughter of a worldwide Telefónica network structure. And we have subsidiaries more or less all over Europe.

Brian Contos: Your role at O2 is pretty expansive. Could you give the audience a little bit of an idea what you do at Telefónica O2?

Daniel Stricharz: Besides the mobile network services that we offer, Telefónica O2 Germany provides a huge customer portal. For example, we offer of course the customer to check for our products. We have an online shop. And once you are a customer, you can take advantage of several other services that make the life as a mobile customer more fun. There are also services like what we call a communications center, a web-based email solution, where mobile customers are able to sync their address books. And there are some location based services. For example, you could, in case you lose your mobile handset, you could locate your handset over the Internet.

So, there's quite a bunch of services that we provide to our prospects as well as to our customers. And they are quite heavily used. So we have a very popular online portal, and online services, around the mobile service itself.

Brian Contos: That's fantastic. It sounds like there're a lot of very new and innovative services that your organization is offering. Sort of above and beyond some of the services that we tend to see in the United States. I guess we're always a little bit behind in the telephony spectrum, when it comes to the new fun things. In terms of web application firewalls, and of course O2 is a customer of Imperva, and leverages our SecureSphere Web Application Firewall, what was the driver behind saying "yes," we need to leverage our web application firewall for our solution. This is a definite requirement?

Daniel Stricharz: Actually, that's a quite long and maybe even complicated story. First, of course, there is the use of legislation in Germany as well as in Europe regarding data protection. There are a lot of customer protection laws. And there are laws that dictate what a telecommunications company has, should, must do or not do. And besides all the legislation, we know that we deal with quite sensitive data. First, all the customer detail regarding his contract information. Then his communication data. All the data that he gives us entrusting us that we deal with proper sensitivity.

So, when doing more than just offering telephony services, such as we do with our online portal, we need to take care that every single customer can not only trust us, but be perfectly sure that his data is safe with us. And of course, on the other hand, we need to protect our own assets. The portal is not only a service to the customer, but of course it serves as a business. We make quite a lot of very serious business over the portal. And as such we need to be in step with what the risks that currently exist are.

So, in the past, we have the same base as I believe as most companies that at some point decided to be present in the Internet, as we called the Web. We initially took measures against what we today call traditional network security. And for the risks that are new to our online world, they are not only found in physical network attacks, but in attacks to the business logic and attacks against the customers.

We are looking always into ways how to protect not only our portal, but our customers. We try to take the same advanced steps and technology as the hackers do.

The question to invest, build up technology like web application firewall was a logical step for us because with those older, now from today's perspective, all the technology we knew

we will not be able to know what is going on in the security world outside and inside our company.

Brian Contos: Daniel, one of the things you mentioned was business logic attacks. More and more often, it's apparent that signature-based web application firewalls and web application firewalls that don't have the ability to learn and understand how both users interact with the web app and how the web app interacts with the database simply don't work. If they don't have that capability to build a baseline, to build a profile, and then identify patterns and/or anomalies, it's very, very difficult to detect, and alert to, and protect from business logic attacks.

I would just like to hear from you your definition of what you feel are some of the business logic risks related to your organization.

Daniel Stricharz: First of all, I need to mention that we have a history with other web-based security measures as well, that we're signature-based only. We saw that that would not lead to the solutions that we required by analyzing locked file errors in applications. Often, we do not know whether some peculiar information in the locked file is due to a security attack, an attempt to exploit whatever, or is it simply an application error.

Since our business is very dynamic, we have a lot of software releases on our portal, and there's some massive code that has been changed all of the time. We need to have lots and lots of knowledge about how to adapt signatures.

After a while, you realize this is not possible, so you need something that not only is more dynamic than a signature, but you need the proper tools that allow you to define those things.

Of course, once you know that, you realize again the sheer amount of data that you have to deal with. You cannot cope with it. In that respect, the application profiling that SecureSphere provides is a huge help because it allows you flexibility. You have three profiles' data, and then just focus on the areas that are most important to you and learn more about the application and content even more than the developer would know.

So, in that respect, the profiling is very helpful for us. It also allows us to apply very specific policy rules in areas where we know that development would either cost us a lot of money, or would take a lot of time, or where there is historic code which no one knows how to deal with at the moment.

So, in that respect, application profiling would tell us, "This is how the application behaves. This is the normal data flow. And here is an area where we need to look into and may even learn that we need to do a security assessment in the specific area because we see something that we didn't know it would behave like that." And then finally we are able to define proper policies.

Brian Contos: Daniel that is very interesting, the picture you drew from using it as an active security tool, but then again leveraging it with the application developers for analysis to actually see how the programs are working. Great use cases. Could you drill down a little bit and maybe share some of your experiences using Imperva SecureSphere WAF in terms of some interesting things that you might have discovered while using this that took you down one path or another or actually caused you to make code modifications or manipulate network configurations?

Daniel Stricharz: I need to say that it is very important to work closely with developers when you are dealing with a web application firewall with the complexity like the Imperva SecureSphere Web Application Firewall. I am not saying it is complicated, but it is a complex product with complex data flowing through the web application firewall. Now, with the method for portal like we have, we have a lot of data running through the web application firewall.

When deployed initially, we saw a huge amount of ill-behaving requests. We wondered whether those would be just intentionally or unintentional attacks. With the ability to visualize the data in the web application firewall we were able to see quickly that those ill behaving requests are due to either broken browsers, broken home routers that have problems when they do address translation.

We saw that from all the broken data that we see; only a certain amount is potentially related to real security issues. When selecting this ill behaving data and concentrating on real security issues, we, for example, found that there is a form on our portal that has been abused for spamming.

Actually, this is a form where someone can recommend a certain page on our portal to another person, like what you often see on news online portals where you recommend a certain article to someone else.

By looking at the events and seeing that there are errors regarding parameter link violations, we learned that we have code where the security structures of those forms, as for example, the message body, which we allow to be filled in and should not be longer than a certain amount of characters was violated again, and again, and again.

This was something that the web application firewall showed us, and we were not only able to block that, but to analyze why this was happening, the typical error here that you place the security logic onto the clients, and we saw that someone was abusing this form. The underlying script was bypassing the script that did the security check and posting huge amounts of spam messages to the web server and sending spam to other people.

This is, for example, an area where we only were able to find it with the web application firewall. This is a very special aspect of the web application firewall like we have it here with the Imperva SecureSphere Web Application Firewall.

It's not about logging things. It's not only about having proper signatures or policies. It's also the ability to visualize certain data and focus on the specific data. This is something that we tried to do before with the locked filed analysis, but you never know before someone told you what to look at.

This is where the web application firewall helps us a lot to focus on specific areas. Even if you do not block something, that you are able to create policies that even more focus on what kind of data you want to get out of the request or responses that either the client or the server sent.

This is one of the examples. Other examples are where we see huge amounts of traffic suddenly against certain web pages, certain forms. Again, initially, the visualization, where a human interface, a person administering the system, is able to take this data, go to a developer, discuss this with the developer.

We even went so far that we gave some key developers lead access to the web application firewall to learn about their own application. It's always interesting to see how impressed the developers are when they see how their own application behaves.

Brian Contos: I think you said it best earlier when you said it's so important to get the developers and the security team working synergistically on these types of projects, because there is complex information flowing through the web application firewall. When you do get that camaraderie, these types of vulnerabilities and these types of risks become much more prevalent, and it's easier to address. It's just very, very difficult to even see them without a web application firewall.

Daniel Stricharz: In fact, I was going to say that if you want to get the most out of the web application firewall, you need to get into contact with the developer at an early stage. The web application firewall from the server is a good opportunity to close this traditional gap between security operations and development. I don't know whether I mentioned this before. I myself am in a technology development department. We are developing the portal, and I'm designing security solutions around applications or doing security design within the application.

So, I'm already trying to close the gap from a security design perspective, bringing security operations and the application developers very close together. Because too often I see, not only because there's some kind of business process in our company, but I hear that from my colleagues in other companies as well, there's quite often a very huge gap between security operation people and the developers.

The people tend not to talk to each other. Why? Because security is typically a pain and developers want to bring their applications into life. They believe they hinder each other.

So, if you have the proper tools, you are able to fill this gap and let those people finally work together, and not after the accident happens, but rather before.

Brian Contos: Well said. Well, Daniel, as we close up here, is there any advice that you can give our listeners out there that are perhaps looking into making a purchase of a web application firewall, or looking to deploy a web application firewall?

Daniel Stricharz: One of the most important points is to either know very well what your infrastructure looks like, or if you do not know about all the details of your own infrastructure, or you have a very diverse infrastructure, look into these opportunities to be able to deploy the web application firewall or even several web application firewalls in diverse methods - so either in-line, or as a proxy, or a router. That was one of the key aspects driving me to Imperva SecureSphere Web Application Firewall. The other point is you should not look too much into the policies and the signatures, or the amount of policies and signatures, but the way of how are you able to work with it. Are you able to bring other people into the mold of properly and regularly working with the product itself?

It should not be something that creates another pain. This is a typical sentiment with a security product. They typically bring more problems than they should.

After all, the web application firewall should resolve your security problems, so it must be very flexible. It must have the proper interface to a human being. It should allow you to communicate the problems or proper reporting for the visualizations.

Finally, it should be very, very granular, what's reported. Either you block properly, or you know what should be your next step in development. If you look at those things and do not

WAF and VA Unite with Jeremiah Grossman

forget that human beings are the persons who work with the device, then I think there are not too many products out in the industry that fulfill that requirement.

Brian Contos: Well, Daniel, that's great advice. I know it's getting late in Germany, so I want to thank you so much for joining us on today's podcast.

Daniel Stricharz: You're welcome, and it was a great pleasure to talk to you.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200