Youtube Link: https://youtu.be/B-4zJaZ6GpA
Resources Page:
https://wpengine.com/resources/webinar-security-proven-ways-to-protect-your-site/

LEXI MOSTEK:
Alright, everyone! I'm gonna kick us off. Welcome to our October webinar. We played a little Michael Jackson, you know. Spooky season, Halloween. I hope everyone was dancing at home. I'm Lexi. If you're new to our webinars, I kick us off, and then I'm gonna disappear. Thank you to everyone that is here on this Wednesday. Roughly, 500 of you. That's amazing. We've got a lot to talk about and only 60 min.

So first and foremost, just some housekeeping things. One. Yes, this webinar will be recorded if you're registered, which you are because you're here, we will send that recording out over email likely later today or tomorrow morning for some of you. It will also be posted to our resources page on wpengine.com. And it goes on our Youtube, so lots of places to rewatch. In addition to that, we do link out the transcripts. So we've got a great panel full of experts here, and anything they name, drop or any programs they mentioned, we will link those out. So don't worry about trying to take notes or do anything there.

Next thing we will be taking questions during the webinar, please, if you have questions put them in the chat, or we prefer in the question and answer section that way, we can filter through them and grab them easily to ask our panelists at the end.

Just a real quick recap. Today we're talking about security. But we did do a webinar last month on performance, security and performance and WordPress and on the web are very, very related. So if you want to check out that webinar, a lot of the things we mentioned today were also applicable in the September webinar. And you can access that on our website

For a quick agenda. I'm going to hand it over to our host. The lovely Krystal here in just a moment, and she's gonna take you through security 101 like some basics you should need to know, just like a quick list. And then she's just gonna talk about Wp engine offerings in security as a hosting provider. And then what we're all here for is this panel. And we're gonna ask these panel of experts some questions on security and data, privacy and everything in between, and then we will take your questions.

So without further ado, Krystal, I'd love to hand it over to you. Can you introduce yourself. What you do at Wp. And then take us through the rest of the webinar.

KRYSTAL O'CONNOR:
Sure! Hi, everybody! I'm Krystal O'connor, so glad to be behind the mic with you all today and working with this wonderful panel, I'm Krystal O'connor, and I'm senior product manager at WP

Engine, and I work on our edge network platform. So the entry point to a visitor reaching yours site. That's where I live, James, would you like to introduce yourself?

JAMES BROWNE:
Yeah, sure. Hi, everyone. So I'm James Brown. I'm a digital director at Flipside Group in the Uk. As a business. We kind of kind of really embrace. Try kind of the power of tech, and in particular, in terms of digital transformation for all our clients through apps, web kind of ax, client technologies. More recently.

And kind of personally, I focus on the web and API side of what we do for our clients. I come from a developer background. Predominantly. Microsoft technology. So don't all you know, start shouting in the chat and throwing things. But you know, as far as Im concerned here, you know, security. It's kind of the same across all platforms. So got some great stuff to talk about in terms of of my experiences across lots of our big kind of customer facing websites and some of our more kind of hidden clients, but more business to business. So hope you're looking forward to it.

KRYSTAL O'CONNOR:
Excellent! So glad to have you here today. Scott, you're up. Would you like to introduce yourself?

SCOTT JONES:
Sure thing. Hello, everyone. I'm SCOTT JONES. I'm the CEO at Illustrate Digital. I founded the agency around almost 10 years ago, 10 years in December. Which is quite exciting to almost be reaching that milestone. We're an enterprise sort of a specialist agency that works in WordPress.

And we also do user research and user experiences as well. So we're all about creating frustration free and engaging experiences on the web. And that's what we're focused on. We also have recently, or I think, actually, earlier than WP Engine might have done. Joined the Iso 27,001 club which is an international certification for security. So hopefully, I can lean into a little bit of that experience today and share our view.

Krystal O'CONNOR:
Fantastic. Thank you for being here to day. Alain, you're up.

ALAIN SCHLESSER:
Thanks, Krystal. Hi, everyone. My name's Alain Schlesser. I'm the Director of Technology and Innovation with XWP. XWP is a distributed agency for enterprise WordPress headquartered in Australia, but distributed across the globe. I'm a software engineer by trade, currently working more as a general technologist and today, I wanted to share. Some insights about some of the security topics that are often overlooked. and also about data, privacy and data governance, and how that relates to security and what you should be aware of in that regard.

KRYSTAL O'CONNOR:

Fantastic. This is gonna be an awesome conversation. I can't wait to get to it. So let's go ahead and get started. Did you all know, that more than half of all cyber attacks target small businesses a lot of people that I talked to think that this happens to big organizations, because that's what we hear about in the news. Right? But Ddos attacks out of date WordPress themes and plugins. I have a question about that for the panel: SQL injections and cross-site scripting attacks. These kinds of things can happen to small businesses and individual sites as well. So security really is something that's important for us to keep in mind. No matter how big or small we really are.

What are some of the things that you need to be aware of? Security is always evolving, and it's always changing. So keeping up to date on what's happening out in the world and how you can mitigate those attacks is really important.

Maintaining good backups. At WP engine, we do backup your sites for you. But if you're gonna make a change, or if you're trying to fix a thing or update a plugin, maintaining backups is really important, we're gonna talk a little bit about user management. That also is really important. And the impact of insufficient security. What happens when things go wrong?

Change is part of the process. Change from upgrades to updating your knowledge. What are some of the principles of security behind that: confidentiality, confidentiality of data, for example. integrity and availability. The principle of least privilege kind of that idea of need to know or need to have access. Maintaining that least amount of privilege for that user is necessary for them to do whatever it is they need to do. These are all important principles to keep in mind

Updates are vitally important, and we are going to talk about this in our panel today. But WordPress runs on what is often called a “lamp stack” so we're talking about Linux, Apache, or Enginex, Mysql. Php. And it's just important to make sure that you or your host is keeping up to date with things like Mysql and Php. On the server, just as is important to keep up to date with WordPress and WordPress plugins and WordPress themes.

But before you make those updates make sure you run a **backup**, because if something goes wrong, or maybe there's an incompatibility or something gets a little funky. You wanna make sure that you can always go back and restore that backup before you make any changes. Always backup your site.

What about user management? User management is really important, not just because of maintaining your your circle, so to say, but also because if an attack were to happen, what can be, what can that user be used to do a thing. So we wanna make sure that we're using really strong passwords so that a password can't be guessed. And maybe somebody with administrative privileges is suddenly used as a vector into your site.

2 factor authentication. We get notified to use 2 factor authentication on so many sites and web applications. Today, it's just as important on your site to help keep those users secure.

Change your login path. So site.com/wplogin. change that to something like site.com slash some obscure name here. So it's not so easy to guess and monitor your user activity. Gee, I thought that person was on vacation all week, but they seemed to be logging into the site, pretty often. I wonder what's going on there? Just monitoring that activity and making sure that it seems normal, and making sure that your users have the right privilege for the job they need to do.

Pick a good partner. Who you are hosting your site with, can help make sure things like Mysql and Php. Stay up to date. They may even be able to help you with things like WordPress upgrades and Plugin upgrades to make sure that it's really easy for you to stay up to date. Or maybe they're providing you with automated daily or nightly backups, all very important, maintaining Ssl certificates, web application firewalls in case you were wondering what WAF stood for. Even third party audits. These are all really important, and your host can help you with those things.

What is the impact of a security breach? If something were to actually happen to your site. How can that affect you? It can affect you in a number of ways from brand impact and trust or identity theft. If there is a data leak as part of the attack here. In that case. Data loss. For example, if you have to restore Backup in order to mitigate an attack on your site? Do you lose orders that are stored in your database because you're now going back to a period before and just generally business disruption which can cost time and money.

Taking a look at WP Engine and security overview

Site maintenance is site security. So if you look at that circle there on the right hand side. Vulnerabilities by component, WordPress. Actually, it takes the smallest amount of the pie. WordPress itself isn't too shabby. Themes are around. 5% Plugins are 92% as a vector to security problems on your site.

So how do you manage that offerings such as the Smart Plugin manager which will back up your site and then automatically update plugins that can be updated. So really, great way to help stay on top of plugin updates. WP Engine also runs vulnerability. Scans will notify you if it detects that a Plugin exists on your site that has a known vulnerability. So you can take action.

We also maintain Mysql, Php for you automatically will let you know when upgrades are coming and you can choose your Php version right in the user portal, making sure you're staying on a secure version, and they also do WordPress updates to make sure you're up to date with the most secure version.

Leave WordPress security to the experts. So we're gonna talk a little bit about

Starting at the entry point all the way down into the application. And here you're looking at the attacks or or just general traffic coming in through the network and then down into the application. So we offer global edge security, which is an add on over at Wp engine and global

edge security offers managed web application firewall and advanced Ddos protection. We're gonna get into a little bit about Ddos. What that is, and what kind of symptoms do you notice on your site when it happens?

The web application firewalls can help mitigate that. And global Edge security. As an add-on offers that as a solution to help mitigate those potential attacks.

Alright. So again, Hi, I'm Krystal, and we have James Scott and Alain joining us today, we're gonna have a fantastic conversation. Let's see, Yup, we're gonna have a fantastic conversation about security today. So, Hello, friends, how are you all today?

JAMES BROWNE:
Really good. Thank you. Thank you for inviting me here.

KRYSTAL O'CONNOR:
absolutely so glad to have you all here. So the first thing that I want to talk about today is we're talking about security for our WordPress websites. But security doesn't just start and stop with WordPress itself. We just talked about a couple of different things from networks to Php, and and my SQL, it's really multi-faceted. Let's talk about some of those areas or layers of which we need to be thinking about security. James, would you like to start us off today?

JAMES BROWNE:
Yeah, sure. So, as you say, stay, you know, app. The application is what everyone sees. Ultimately they like the browser. They like the app, and they see a website. So they assume that that is the product right? As you say, there are so many layers before that product, if you like, is even delivered to an end. User. So you know, since that request is made for for URL, for example. it's likely to go through as you said, maybe Cloudflare or economize other products offering an edge service for protection against kind of dollar service attacks or any other kind of kind of bad bad player kind of traffic and then through various caching through various other systems, middleware, etc., etc., which all have a part to play in the security profile of of your product.

So, for from you know my experience, you know, we work a lot with with Akamai so often very similar services to Cloudflare and you know that's where we like to make sure that there is, you know, huge amount of security. There, that's your front door right? That's you know. You don't leave your front of your house open or your windows open. Right? So you know that that's what you're looking at, making sure that as much as then bad traffic is stopped there. And you know those tools have so many, so many features built into them that you don't really need to do much, you know you you install, and you pay right and then and then you configure as you go.

SCOTT JONES:
James. Someone shared an analogy with me a while ago around. I mean, not that I hadn't seen those stats around the number of logins versus sorry the percentage of plugins versus you know

WordPress itself, which is, which is quite good to see actually, cause it does match what we see as an agency and sort of thing that we end up dealing with and looking after.

But someone gave me analogy of it's like having more windows in your house, and the more windows you have the more entry points there are to break in through. So, generally you want to keep the number of plugins that you've got to a minimum on that way you can take more control of the issues that might occur with those plugins, the updates on those plugins. But also, you know that the things like you said before that those plugins actually have control over and and doors into within the rest of the website.

And third party you know, platforms as well.

ALAIN SCHLESSER:
Yeah, definitely, you want to reduce the surface that is possible for attack as much as possible, and probably with with the layers like the network layer. And then the physical layers, the application layer. You can basically think about it like a negative marketing funnel, like with a marketing funnel. You have a larger starting base, and it gets narrow and narrower as you go down.

Just the point with the security funnel is that you want to have the least amount of people ending up at the bottom of the funnel instead of the most amount of people. So ideally. The first layer is the one that filters out the most because it's also the cheapest one to filter out in terms of resources needed. And it's also the one that gives the least amount of potential for further breakage when it's being pummeled by Ddos attacks or something like that.

So you don't want to have bad actors hitting your server as much as possible, so ideally get rid of them at the network level straight away. So your server is never even aware of it. So you don't need to prepare your application server for that scenario at all.

SCOTT JONES:
I'm just thinking if I'm really Krystal about zoom, Zoom announced a little bit further. You said, you know that the security doesn't necessarily start with the websites, or with WordPress, or or indeed with WP Engine. And if you zoom out to the wider business and the business relationship, whether that's an internal IT or development team, you know, and the marketing team, or whether that's a freelancer and that client or an agency. And that client. You know, II think the accountability between the 2 sides is really important there, and actually understanding and being clear with each other about who is looking after what you know is is the agency looking after? You know the Dns and the cloudflare, and and that aspect. And is it our responsibility to update plugins? Or is it? Is it something you're gonna do? Just making sure that you've got every single base covered and almost right yourself a checklist of all the things that you should do every time that you launch new site or work with a new client. You know, having that.

I'm not. I'm not a fan of having too much process, and it can get in the way of progress sometimes, but actually having some of those processes that make sure you take the boxes, particularly from an accountability and conversation perspective, it can really help to stop those gaps from actually appearing.

You know, later on down the funnel, that Alain's talking about that you know. So that yes, actually the right person updated the plugins at the time. They said they would or you know, the the cloud flow set. So it was done correctly, or WP Engine relationship was owned, or or whatever that may be, but that, you know, goes goes across an entire business or an entire you know, freelance. You know book, if you like. Not just a specific website or specific instance.

JAMES BROWNE:
Yeah, it does, were so used to these days to building sites kinda like mobile. First, for example, everyone knows that phrase, yeah. And it's the same with security. Right? Security needs to be first, you know you, you know there, there's so many house analogies, you know that you can pull people with. But you don't start building a house by the roof. Right? You start the foundations, and that's all these things that you that Scott was just talking about in terms of those processes. And who's responsible? They're your foundations of any site you build, and you get those right. You get those in place, and everyone's on board with those you know. Whatever you build on top of those you know might not be what customers want. It might look shocking, but at least maybe she could be secure.

KRYSTAL O'CONNOR:
We're really talking about security is a mindset, and making and building habits and building a muscle around that and inside yourself and inside your organization. Right?

JAMES BROWNE:
I think ha historically, I think security always, I would say historically on, you know I mean my forties now. So I'm talking right back at the beginning of building websites. Security. What people didn't think of security, you know, they built websites. They threw it up. They didn't really kind of think about what people would then do to that data that was being collected, or you know how it could be impacted. And you know, it's so important, not, you know, for many years. But you know particularly you know, at the moment, with lots of kind of big, big kind of tax going on, and stuff, you know, there's lots to consider.

ALAIN SCHLESSER:
that's an interesting point. So if I think back about how yeah. In the olden days websites were built. So mostly the application was not really an application at that time was mostly static HTML, with some Cms Css. That you've built. and now with the way a modern web application is built. It's really much more like a full client-server application. Where there's so many interconnected pieces that communicate with each other. And so the security needs to happen, not only at the web serving end, so that you just need to secure your lampstack, but you actually need to secure all the communication that's happening between these components.

Which is another area of the network layer that needs to be secured as compared to when you just had a studying at HTML site. So once your web server was secure, you were were good nowadays, being. While your application is sending requests back and forth between the browser and several different types of service that are probably making up your system. It's getting much more complex to care about that. And you need to really think about a systematic approach to cover that and have rigid processes in place, because otherwise you just lose track of what is happening behind the scenes very easily.

KRYSTAL O'CONNOR:
So let's take a look at that funnel in the top of the funnel. For those who may not be fairly familiar. There's all different kinds of attacks that can happen at the networking layer, things like ping of death attacks. So that's really ominous like it's almost Halloween. Sin flood attacks and and dos, or Ddos. Can we talk a little bit about what a Ddos attack is. And what kind of symptoms might you notice when something like that is happening?

JAMES BROWNE:
Yeah. So I mean, yeah. So I mean, we, one of our clients is constantly under attack, right? So they are a big pizza chain and they're constantly under attack and what we see. And also with all these systems in place. That's before we don't. We don't see them anymore. Re. In reality they happen, but they kind of defended against at at the edge right? But many, many years ago, you know the first we would really realize about this was all. Rs. Would fire off. Everything could go red. We'd have text messages saying CPU was up to 100%. And kind of response times are really slow. And you know everything could be firing off.

And you know everyone kind of jumps on it. And what's wrong? What's wrong? You know service is sluggish. Nothing's no pages are loading and whatever, and start eventually. Then, to kind of look at the picture, get into the logs and realize that. Wow! Wise, my log file. 700 MB now, and it's normally 200, you know what's going on. And yeah, you know, you, you get to the root that there's, you know, massive amounts of traffic and a kind of traditional details which is just kind of, you know. Volume volume led

Huge amount of traffic, maybe to targeted pages which attacks have realized a more kind of resource hungry than others. But generally from, you know, massive spread of IP addresses, big spread of pages, user journey, etc.

And it looks quite. quite drastic. It looks like you know your server is dying.

KRYSTAL O'CONNOR:
It can feel like it, too. Alain, I'm gonna pick on you for this. Let's say I have a site, and it's experiencing a Ddos. What are some things that might have in my hmm. Some might call it a doomsday playbook to help get things back online to to mitigate the situation. But then also, how does it affect my reputation as a brand or as an organization after the fact?

ALAIN SCHLESSER:

yeah. So let me get to the first part of that first.

So with a did us attack usually you want to first mitigate it. Because, you will have time to do any forensics. Any route calls on this later, but the most important part is to be able to properly deflect and mitigate it. In the initial onslaught, because while the attack is happening, chances are good that not only is this, causing a lot of problems, strain and extra cost to your assistance. But also, probably you're not available to your visitors, your clients anymore. So if you're running an e-commerce site. For example, people will not be able to buy anything while this is going on.

So usually there's several ways of deflecting that. But what I recommend generally is that if if you're responsible for an application, for example, if your core business is not managing service. Then you should not be the one trying to do that you should have a strong partner on your site like WP Engine for hosting, for example, where you immediately let WP Engine know, you probably do already. Figure that out. Because they will also have the alerts pop up all of a sudden and then also have systems in place like Cloudflare and Akamai, which have on one hand a protective layer that can also already protect against some of that, and they also have the mechanisms in place to help you immediately Block traffic based on some criteria or reroute traffic to other servers. Adapt the load balancer, and things like that. So there's different ways to to mitigate that immediately, to deflect that

But you should ideally have the systems in place already before that starts. If all you have is a physical server, you're running yourself that you put on the Internet. You're in a really tough spot to be able to properly handle that. So all of these protective systems to properly deal with a serious Ddos attack, they need to be in place upfront. So this needs to be an infrastructure that is already planned and implemented in such a way that you have ways to fight for your server. In in case scenario like that happens, because otherwise there's not you. You can always work on the network on the Dns layer, and things like that. But probably if you didn't plan for that you will not get to a point where your visitors and your clients can get access to serve a while. This is ongoing.

You can just basically take your server offline and wait for it to stop. That's mostly what you can do in such a scenario.

JAMES BROWNE:
because because you can't even put up a sorry. We'll be back later. Otherwise you're in. In a really tough spot.

ALAIN SCHLESSER:
Then, in case something like that happens. So, for example, being offline for several hours, or even worse. Can have an immediate negative impact on your business, of course.

And, also, you need to consider that nowadays people are being more more aware of what a security breach means, what that, what that might entail. And even if nothing bad actually

happens, apart from being offline. People will already have doubts about what the impact has been behind the scenes, and you will also have a hit on your reputation, even if it's unwarranted. So this is a situation that you'd likely want to avoid, in the first place, by having the means to immediately switch to alternative ways of dealing with the traffic so that you can mostly keep your systems online and available for your clients.

SCOTT JONES:
It's been a genuinely long time since I, as a CEO last heard of any of our clients directly for myself, having an issue with the Ddos attack that made it public, or or had an impact externally. But I guess that's also probably as a result of the WP engine doing such a great job and pro, probably worth talking about. For a second. The rule sets that they have in place compared to, you know, just going and getting an aws instance of your own, and pushing the sites out there and and hoping to self manage it because you know, the the specialism within WordPress that WP Engine has is is the extra little source that we're coming to them. To make sure that that's covered, that any known issues, any known vulnerabilities are covered off and already already taken care of.

And I think you know that tends to be our recommendation is exactly what Alain just said they're around having, you know, a really good hosting provider. And you know, a really good layer of support behind that which, of course, might my team do for our clients? We do a lot of our work in the legal sector financial service sector, Fintech banking you know professional services. Government. So in those industries particularly, it's even more important from a credibility and reputation perspective.

And that's you know, the majority of the time. The conversations we're having around the need for the website, of course, is partly to do with converting potential leads and signing customers and that side of things. But it also is about credibility and reputation. And so you know, the longer website is offline, the worse that gets for their credibility the worst that gets the reputation and people start to ask questions, and if it's there for long enough, the news will pick it up, and it will become a much bigger deal. And it actually needs to be. And and it does start to create those question marks.

So, you know, removing the possibility of of those question marks being created is really what we're trying to do when we're you know, doing all this great security work to get ahead of those issues.

JAMES BROWNE:
Yeah. And that kind of reputational stuff really sticks. And and it is hard then to to I don't mean recover like it's gone forever, but it's hard to get back to where you are to slow process, you know, and you know the kind of Fmcg brands that we work with at flip side.

You know you. Of course you lose that immediate transaction, so that you know that person is not buying at that moment, especially when it's a kind of impulse purchase which some of our customers are. They, you know that you've lost that purchase. But then they've gone to

competitive brand. Then, you know, you potentially lose that customer for that, potentially for their lifetime. Right and over X number of years of that customer buying pizza, for, you know, once a week, you know, it's just a lot of money. So you know, there's a much longer tail in terms of the financial impact. And then we'll see the representational damage off the back of it.

KRYSTAL O'CONNOR:
So we've talked a little bit about the edge, about the networking side of things and and the reputational hit and and other business applications, for if something were to happen at the networking layer. Let's take a little look at the application side of things. We saw a chart earlier that's talked about. Vectors of 3% really coming in on the WordPress application itself? 5% on themes and then 92% on plugins.

Can we speak a little bit about right? Right? Can we speak a little bit about why Plugins are such a vector and what we can do to mitigate that Scott, I'm gonna pick on you to lead that one off?

SCOTT JONES:
Yeah, sure, II guess I mentioned earlier on that. You know it. It's worth initially and periodically auditing the need for plugins. So we tend to try to suggest putting as few as possible on your website if you can. But of course we also understand the beauty of WordPress is its extensibility. So you know, a lot of a lot of WordPress admins out there can go wild on adding and adding and adding plugins. And even when you look at, you know, maybe without naming any of them, you may look at like potentially a form Plugin, and that Plugins got a number of different extensions that you can add to it, and the same for e-commerce. And there's a number of different extensions. So it's very tempting to immediately start to add a high number of plugins for that functionality.

I guess the way I would look at it is, do you really need that functionality? Is that mission critical? Is it conflicting with something else that you are also doing somewhere else? So are you doubling up on functionality? And also, is it possible to do what you're doing with, you know, with hard code, without having to, you know, put too much effort into doing that. So if it's something that you can do without opening another window in the house and it's something that you can do internally. To put it in that perspective, then, you know, definitely try and do it internally, because that's a lot more secure. So you know the initial things that we would say.

But also, there's a few tips, I guess, that you can look at in terms of when you're choosing and selecting those plugin. And so the couple of things I think you wanna look at are or maybe 3 things you wanna look at is who was the developer of that plugin? Do they have a degree of reputation in the industry? Is it the brand themselves, and if it's the brand themselves, then then that's a pretty good sign. Usually, you know, if you're putting a review plug in on the website. And it's from that review brand it. It's usually, you know, a good one to trust.

The second thing is, how many reviews does it actually have on that plugin in the repository and the WordPress repository? So you know, are people saying good things bad things about that

Plugin, particularly and the third one would be, I'm probably the most important one. When was it last updated? And what version number is it relevant for so if you look at a plugin that's got 5 stars. But it was only updated 2 years ago. Probably want to avoid it because no one's looked at it, tested it, and made sure it's not vulnerable in the last 2 years. Which is not a good sign at all. In fact, the good practice would be.

If you operate a plugin and you haven't had any vulnerability opportunities in the last 2 years. Just do a small update, anyway. Because showing that you've actually tested it and run an update recently is A is a pretty good sign. So it's a few different things that you can do to make sure that you are. You are you treating Plugins well, but just audit them regularly as well. Go back to them. Don't forget about them. Make sure that you're you know, ensuring that you've got the right sets of plugins actually install to begin with.

JAMES BROWNE:
Yeah, III think, because they're easy to install. And then this kind of whole kind of library from people, I think, assume that they all work, and they're always good at each other, and it doesn't really matter what I add, because I can add it, you know, and like you say, Scott, that you need, you need to work out whether they are needed. And they need to kind of fight their own corner, right? They need to prove that they needed. And yeah, you know.

There's crazy stories of, you know, Javascript libraries where you've got plugins that are, you know, is this number odd, you know. And you know, I'm sure that's a joke. That Plugin. But you know you know, the the point remains that you know there are some plugins which do actually under the has some very simple things that you could do yourself, and therefore you haven't opened yourself up, or you say, Oh, you haven't opened another window of attack.

ALAIN SCHLESSER:
I just want to quickly note that there's no technical answer to the question, how many plugins is too much or or too few. Well, too few will not never have too few plugins. But so technically, All that happens is that there's a Php file being loaded. So having 1,000 plugins or having a thousand Php files in one Plugin doesn't make any difference. It's not the exact number for technical reasons, but having a thousand different plugins on your website, it can. Technically, it can run just fine. But you're making

1,000 bets of every single one of these plugins being flawless in their security practices. And if you combine that with the fact that a lot of the WordPress ecosystem is grown out of hobbies, ambitions, and not out of serious engineering practices. It is this. But if you make it too many times, there's actually high probability of being wrong at least once, and that is enough to cause real issues.

At XWP. We generally try to have as few plugins as possible, but not only for security reasons, but also for scalability reasons, because at a certain level of scale, you quickly find out that almost all plugins in the WordPress space are just not built in a very scalable way. So there's

other other issues that you notice with plugins. So we tend to custom code most of the functionality, anyway.

But just note that it's not the number per se. That is the problem. It is how many untrusted dependencies you're adding to your site.

KRYSTAL O'CONNOR:
So let's say, I have a bad actor who notices that I've got some bad plugins or outdated plugins or outdated software. And I find my way into the system. There's a number of different things that could happen from, you know. Maybe they make your front page look a little silly, and so you restore backup all the way to things as scary as a data breach.

So when we have the concern of a data breach, what are some of the first things that we need to be thinking about again coming to that playbook of mitigation. But also, how do we further protect our reputation, but also the data of our customers? At that point, when we're dealing with something like a data breach.

SCOTT JONES:
If I could take that a few steps earlier than when the breach occurred. Ii think one of the things that I would be recommending that any individual or business do is actually get someone else that party in to have a look and do some level of audit. Because I think it's actually really important. And it doesn't necessarily matter whether that's super detailed like Iso, or whether that's quite surface level, like a friend. Come in and poking around it, you know it. It depends on, you know, the level of severity, the size of business, that sort of thing.

But the reason I'm going back to that stage and recommending this is because it's really good to be exposed in a safe environment before you're exposed to the rest of the world.

And so actually to force some of that exposure and to see some of the potential issues. And some of the, you know, the areas that would be vulnerable, the sort of data that could get out. It's really important to understand what that is early on rather than waiting for something to go wrong. And then realizing, Oh, my goodness, that's definitely something I didn't want the world to see. You know.

So I think I would take it from that perspective. And maybe the other guys are better answering the what to do once it's happened so far.

ALAIN SCHLESSER:
Yeah, I'd also like to first take it a bit earlier. And that just 2 things I want to mention here at a time to what you just said, Scott.

One thing is that - It's really important to actually be exposed, as you said. So, for example, the best backup in the world will not help you in any way. If the recovery actually doesn't work, and a lot of sites never test their recovery process. So they religiously create backups and think

they're safe. But you're only safe. If you actually test whether it helps you in the case of a problem, and it's the same with security. So all the security practices you put in place. If you never let someone else try to actually get past them, you don't know whether they work or not. It might just be that you have some Bennetti metrics and checklists filled out? But you left the door open in some other area, so these things need to be directly tested by a third party to make sure that you didn't miss something obvious, and that your practices actually work as expected.

Then, in the case of a data breach. it is before talking about what you're supposed to do, then it's important to know that the data breach is something that all the security best practices try to reduce the probability of that occurring in the first place. But they don't. There's never any guarantee you're just lowering the probability of that happen.

And there's still a remaining percentage of probability that it will happen. And that's where the preparations come into play of how to minimize the impact of a potential data breach.

Because, as you cannot fully secure yourself against a data breach, as there's always the theoretical possibility of it happening. You also should work on minimizing the impact of a data breach. That's where data, privacy and data government governance come into play, in the security context, you can think about all the data that you're collecting. So this is again. I think we're at the same space here. Where this is the negative of the marketing approach. So in marketing all the data that you're collecting, it's pure value you want to have as much data as possible.

In terms of security, data is a liability. And you actually want to reduce the amount of data that you have, you run to reduce the amount of liability that you're collecting. Because every data breach that will happen will directly be multiplied by the amount of data that you made accessible through that data breach. So if you start by not collecting data that is not needed, if you start by anonymizing. And so then I so you don't need complicated work all the data that that you don't need in the raw form. You can actually minimize the liability that you're exposing yourself to in the case of a data breach.

JAMES BROWNE:
Yeah. And it's that classic. I suppose idea of, you know, if you leave things visible in a window is gonna make it more attractive to someone to try and steal them right. So you know, if you've got a form and you're collecting, you know, 27 attributes about a customer.

An attack is, gonna look at and think. Well, that's some really valuable data. If you're just collecting their kind of name and hair color, for example, that's not much use to anyone. So you know, it comes back to that. Do you really need someone's date to birth? Do you really need to know? Kind of, you know, address details, or you know, whatever kind of information you need, and it really then reduces, reduces and reduces the value and the kind of desire for someone to attack and maybe steal that data.
You know. And the process, you know, if the worst thing you know has happened, you know, I think I think there's various steps you go through in there. This kind of technical steps and

process steps right? So you know, it's a moment to panic. But don't panic, right? Cause you know you. You need to keep a level head, you know, and a lot of it comes down to logging times findings as you're going through logs as you're going through systems that may have been breached. You know.

What is the state of that system at that point in time tracking that time. What did you find? What's wrong? What isn't wrong? It's really kind of forensically going through access logs. And you know who locked in who didn't log in, you know, who made update. He didn't main update, you know, all the kind of things you'd go through as you kind of like kind of yes, I forensically going through everything. you know, and ultimately trying to get to a position where you're trying to find out what happened.

You know. And you know, say this technical things you can do in terms of maybe putting up a holding page. If you think there's something you know. Wrong with a web. Everything particularl URL, that's just giving out data. You know, you can put a holding page. You can turn off the that particular site, if you need to, you know changing passwords to service. If you think that the kind of leak has come from an internal source. You know, so you can go through all these steps.

But I think the key thing is to really kind of keep a level head. You know, it's happened. It's bad. There's gonna be repercussions. But you know, you need to make it stop. There's nothing, you know. Don't panic.

ALAIN SCHLESSER:
Yeah, there's also I'm sorry.

KRYSTAL O'CONNOR:
I was just gonna say in the interest of time I'd I'd love to get some of our customer questions Lexi and Luis have have given us a pretty long list here. So I'm gonna pick a couple and get your opinions on some of these. So the first one here how to implement a serious content, security policy, or a Csp. Without breaking WordPress. Too many exceptions have to be put in place if it's serious, but then that makes it hard for WordPress to actually work.

So what are your thoughts on on the balance between security and functionality?

ALAIN SCHLESSER:
There's a definitely a lot of areas in stock WordPress that could be built in a better way to make it easier to combine them with proper security practices.

Generally, there's always ways of of doing that. But, for example, if we're talking about WordPress back end. It is already behind an authentication wall. So probably you should start by separating your Csp policies between what you're doing on the front end and what you're doing on the back end in some way. That makes it easier to reason about these 2 different contexts and what you need to consider for them separately.

And then on the back end. You are. You are free to adapt in necessary ways, but also the back end can be secured in in additional ways to make the network space for the back end safer. So you can, for example, build a system where the front end is accessible to the public world wide web. But your back end is not the so. There's different ways of going about that, depending on how far you want to take it.

You can have a demilitarized zone. You can have a VPN only access things like that, but generally consider the WordPress back end to be separate from WordPress front end, even though they are being served by the same application. They are different security contacts.

KRYSTAL O'CONNOR:
So the next one Scott, if you don't mind, I'm gonna throw this one your way. I've seen this one asked a number of times does disabling a plugin in WordPress, do the same thing as removing it or deleting it? Are they the same?

SCOTT JONES:
Oh, my days! I am totally not technical enough to to answer that question properly. So I'm gonna I'm gonna Bounce Pass, either of you like to take that one.

JAMES BROWNE:
Yeah, relatively limited. But I mean just thinking of. Generally it helps to disable it. But I it doesn't do the job right, you know, disabling it stops it from functioning and and in. If the module of a plugin is built correctly, it's fine. But again, you're at that risk of knowing. Did the person who built the Plugin actually kind of build it properly. And are there other files that potentially still accessible? Even though the plugin has been disabled?

But but yeah, I mean, and then you you probably have better answer for that.

ALAIN SCHLESSER:
Yeah, in terms of security disabling and deleting is 2 very different things disabling just means that it is not being loaded by WordPress by default. But the files are still present on the web server, and depending on what those files are, and how the web server is configured. This can lead to all sorts of problems. So first of all, you can any static resource, will still be available on its URL in the Content folder, for example, because that folder is by its very nature publicly accessible, at least, if you know the exact URL of these files.

And then depending on how the Web service configured. If the web service misconfigured, it can even lead to direct code execution of the plugin that would mean the plugin is bad, and web server is badly configured. So you have more problems than not just deleting the plugin, but it means that in such a case disabling the Plugin will not remove any of the security issues. They will still be there as long as these files are present on, so that it can be remotely executed. Whatever the initial issue was, so disabling. Has no impact on the files that are available through the web. Disabling just means that WordPress will not execute these Php files in its normal execution flow

SCOTT JONES:
For what it's worth. I knew the answer was delete. I'm just not smart enough to explain why.

KRYSTAL O'CONNOR:
The next one is a little more, a little more, general, and it's related to backups that the original question was, are the backups stored on a separate server? I'm gonna reward that a little bit.

Is there a difference or an importance behind storing backups off site versus storing backups on the same server where your website is. James, I saw you nodding. So I'm gonna throw that your way.

JAMES BROWNE:
We all nodded, we all nodded, The point of a backup is to have a kind of point in time, kind of freeze frame of where you were when that backup was taken. If that backup stored on your server and your server is compromised via you know any any means, then you know that backup then becomes potentially at risk, right? So whether you know removed or whatever and what it also means is, if you, if you, if your system is compromised, but you don't know. It's been compromised yet, and your backup still keep running

Your backup now includes that, you know whatever was compromised potentially so keeping something off site secures you against any kind of security issues that you have in that server, but also any kind of disaster scenarios where you know that server in that particular geocation goes down. I don't know if the data center disappears overnight, whatever. You know. You've then still got your backup in a completely different site. you know. And you can then kind of maintain your service via using that backup

KRYSTAL O'CONNOR:
and one final one for today as a small business administrator in house, do you have a source on how to do an inventory of plugins? Or I'll add how to do an inventory in general of your site - anyone to take that one?

SCOTT JONES:
from a simple level, and maybe someone else. The details. So does obviously log into the WordPress backend. As long as you're an admin, or have access privileges to plugins, you should be able to see plugins and it gives you a very simple list of what are the plugins that are installed while the status of those plugins, all those plugins enable? Disabled? Do they need updates?

That's all the simple place to sort of have a view of that. The other place you can go and look, I think, is under tools and site health. And that's a really good tool to run to have a look at. You know what is the basic health of your sites at this point in time which is really useful information to be able to give to a developer or an agency to then do something potentially more useful with

and the other thing that I guess you could also do is run a third party system. So for example, managewp is a is a good one. I'm sure there are other tools available. Both those sorts of tools will help you to sort of have a window into the site at any point in time as to what needs update in what's the performance like? I don't know. The WP Engine sort of got some tooling in that in that sense as well.

KRYSTAL O'CONNOR:
There you go. I'm going to go around my virtual room here and ask one by one if there's any closing thoughts. Alain, do you have any closing thoughts you'd like to provide to the audience today.

ALAIN SCHLESSER:
Yeah, I'd say, I have 2 general recommendations. Try to outsource as much as you can of X, of your security, A few security problems to experts in the field. It's not your core business, so you shouldn't deal with it if you can avoid it. Let experts do the hard stuff, and then always consider the impact of adding more to your site. Be it more data or more code, considered, impact the implications in the long term of what that means, and see it always as a trade off. Everything you do on your website is a trade-off. You're not just winning a new feature. You're trading, yo, you're doing a trade off between one new feature versus one new security, liability, or something like that. So always consider the impact.

SCOTT JONES:
Yeah, I was, I was just thinking of the same thing around. The type of conversation I have with my clients is, and that we have with our clients as an agency. Illustrate, digital is around compromise, and that can be sometimes maybe a negative word to use. But I think it's a powerful one in this case, where we're actually saying to make a decision like this, you're compromising this

And actually to try and find the balance between the 2 different areas. You know, wanna add this feature. But it could create some performance issues, security issues, whatever that may be, I would say, don't be afraid to use the word compromise because it is important to try to find the right answer and the balance between the 2? Is it commercially more sensible, but creates more risk, and therefore commercially less sensible? And you know what? What is the output of those 2 things?

JAMES BROWNE:
Yeah, I think my kind of final words that you know, this whole subject can be quite quite scary is lots of acronyms. There's lots of different types of tech, you know. There's all sorts of negative kind of things going on here.

I think if you look at it, a kind of more simple approach. You can really apply it to what you do in your own life. Right? You lock your front door, you lock your laptop when you walk away. You have a strong password, you, you know you. You go through all those things in your own life, and how you live your own life. And you know, if you apply lots of those same principles to how

you build your network and your websites and applications. You know. That's a lot of the work done for you. But II completely agree with the using experts in their fields. You know, we can all do a job in security. But there are people that are actually, you know, experts in it and use them.

KRYSTAL O'CONNOR:
I just want to say it's been an absolute pleasure talking with you all today. Thank you so much for joining and for allowing me to play along, Lexi. I'm going to turn it back over to you today.

LEXI MOSTEK:
Yes, thank you so much. This is an amazing panel, and I think I can speak for everyone. It was fun like I'm here giggling and laughing and agreeing and nodding my head. But we also had an unprecedented amount of questions. So thank you to everyone that joined, keep an eye out for some follow up and the recording and also we'll see if we can crank out some additional resources. To answer some of the outstanding questions. Thank you. All happy. Wednesday.