Security.Everywhere
Interview with Jack Danahy

We talk at IBM a lot about the smarter planet, and actually what makes the planet smarter is software. And it is fueling some of the most critical parts of most businesses.

The more ways in which we allow people to access systems -- and sometimes these are systems which were never originally intended to be accessed by a broad group of people -- the more we increase the risk.

The very worst thing that one can have happen is to have an incredibly insecure piece of software function perfectly well in all other regards. It's continuing to offer up that insecurity, and so the costs associated are very high.

We know from research that's been done, as an example by the Ponemon Institute, that the average cost of a breach, the entire event, is around $6 million.

But we have seen research done in the automotive industry which showed that when software can be corrupted, they can engage the brakes on an automobile in a test scenario going 40 miles an hour.

And so it changes fundamentally the way we think about the impact of software security problems.

The very first step in doing what we at IBM call being Secure By Design is about learning what security means—What's the application supposed to be doing? What's the business that it's supposed to be driving?

We have seen so much benefit in organizations just through that process of sort of accounting for all the software that exists.

And then, how do I get the organization that cared about security as a business objective, to care about security as a developer's day job?

If it changes the way that people do their everyday job, it can be very hard to get broad, positive adoption.

By integrating within the development environment tools that people are already very familiar with, the Rational AppScan family of products really decreases that sense of disruption.

A developer is using the tools they have always used. They are just getting new kinds of information. And that new kind of information is about security.

The AppScan Source Edition will actually look at the source code, identify whether or not you are doing things the way in which policy dictates you should -- whether you are using enablers that you should -- and also whether you are making any sort of fundamental mistakes in programming that might cause the application to be vulnerable.

As opposed to having each developer focus their attention on the way they think a problem should be solved -- which, by the way, in some cases can cause something else to become less secure -- I am going to run a consistent set of rules against every build, and so I will have a consistent baseline and then progress trends of what's happened inside that application.

So the businesspeople can, number one, make sure that they are getting what they ask for. Number two, in cases of highly regulated environments, they can show trends, they can show the fact that they are looking for the types of security problems which could be an issue, and they can do it automatically.

We have a great example of an organization which had had a security problem relating to credit card data.

They brought the Rational AppScan product in in order to be able to assess one of the critical applications that was very publicly exposed.

The following day -- which was a Friday -- they engaged a team of offshore developers to fix a series of vulnerabilities that had been found through this analysis, which before Monday morning had been updated and released to 3,000 point-of-sale terminals.

This capability of combining super useful tooling in a format that developers and managers and architects can understand, with really current information about the nature of the threat in the wild, is unique to IBM.

And it's a way in which we can combine the best of understanding what goes wrong with the best of understanding how to make sure that it doesn't.