Read or listen to this article online

Scan the QR code to open this article on XO.PL

Article source:

https://xo.pl/it-made-fun-sec-basics

IT SECURITY

IT security basics: why everything will be fine is not a security strategy

On the day of the grand opening of the Manager's new headquarters, reporters, inspectors, security guards and firefighters gathered outside. A huge banner declared: **THE ABSOLUTE SECURITY CENTRE — 100% GUARANTEED!** The Manager was determined to prove that his company was immune to break-ins, malware, outages, thieves, mistakes and, apparently, common sense. Greg arrived carrying a folder of documents and a sandwich. One of them might get him through the day. 🤣

We'll cut the ribbon as soon as we can open the door

— LADIES AND GENTLEMEN! — announced the Manager. — TODAY WE OPEN A BUILDING NO UNAUTHORIZED PERSON CAN ENTER!

— What about authorized people? — asked Greg.

— NOT WITHOUT APPROVAL!

— Whose approval?

— MINE!

— And who approves your entry?

— GREG, STOP RUINING MY PRESS CONFERENCE WITH QUESTIONS!

Just then, Agnes from Accounts emerged through a side door.

— Sir, six employees are stuck inside. Access control won't open the doors.

— EXCELLENT! THAT MEANS IT WORKS!

— It won't let them out, either.

— THEN THEY CAN WAIT FOR MY APPROVAL!

— Sir — interrupted the fire officer — emergency exits cannot depend on your personal permission.

— NOT EVEN IN MY OWN BUILDING?!

— Especially not in your building.

Greg put down his sandwich. — And that's our first security lesson. **Protection that prevents people from using a building or escaping safely can become a hazard itself.** IT works the same way: security should support the business, not bring it to a halt.

Three pillars the Manager never ordered

The inspection team gathered in the conference room. On the wall hung a diagram of twenty-seven alarm systems.

— ALL OUR DATA IS SECURE! — declared the Manager.

— What exactly does that mean? — asked the lead inspector.

— NOBODY CAN STEAL IT!

— What if someone changes an invoice from one thousand to one hundred thousand? — asked Agnes.

— THAT'S FORBIDDEN!

— And what if nothing is stolen or changed, but the accounting system is unavailable?

— GREG WILL FIX IT!

— What if Greg is on holiday?

— GREG DOESN'T TAKE HOLIDAYS!

— I have quite a few days saved up, actually.

Information security is often described using three principles: **confidentiality, integrity and availability**, known together as the **CIA triad**. **Confidentiality** protects information from unauthorized disclosure. **Integrity** protects its accuracy and guards against unauthorized alteration. **Availability** means authorized people can access information and services when needed. Protecting one at the total expense of the others is usually a bad bargain.

— WHAT IF WE PUT ALL DOCUMENTS IN A SAFE AND POUR CONCRETE OVER IT?!

— Confidentiality might improve — Greg admitted.

— HA! I KNEW IT!

— Availability would drop to something resembling an archaeological dig.

— THEN BUY A JACKHAMMER!

— Congratulations. You've invented data recovery by construction equipment.

The hacker with a briefcase and no balaclava

An authorized security tester had also been invited. His task was to examine procedures within a scope agreed with the company. He brought neither a crowbar nor a laptop full of glowing green code. Instead, he carried a briefcase and a badge reading “SERVICE”.

— Good morning. I'm here to inspect the air conditioning. The Manager said I must be let in immediately.

— Could I see the service request? — asked the receptionist.

— He's giving a speech! You mustn't disturb him!

— Then we'll wait.

— The air conditioning could break down!

— We can check the ticketing system. Do you have a reference number?

The tester smiled and produced an inspection form. — Congratulations, you passed. I wanted to see whether invoking the boss's authority could bypass your procedure.

The Manager charged into reception.

— WHERE IS THIS HACKER?!

— Here — said Greg. — We hired him ourselves.

— THEN WHY HASN'T HE STOLEN ANYTHING YET?!

— Because this is an authorized test with agreed boundaries.

— FINE! TELL HIM TO STEAL SOMETHING UNIMPORTANT!

— Sir, an attacker doesn't always know in advance what will turn out to be important.

Attacks do not always begin with breaking encryption. Someone may try to persuade a person to reveal information or perform an unsafe action. That's **social engineering**, and **phishing** is one common form. Good procedures verify identity and authorization rather than trusting a confident voice, urgency or the words “the boss said so”.

Risk gets its own desk

In the Manager's office stood a new armored cabinet. Beside it sat a bucket catching water from a leaking ceiling.

— GREG! WE NEED ANOTHER FIREWALL!

— First, we need a roofer.

— THE ROOF ISN'T CONNECTED TO THE INTERNET!

— Neither are the documents being soaked underneath it.

Security begins by identifying **what matters** (assets), **what could harm it** (threats), **what weaknesses might be exploited** (vulnerabilities) and **what the consequences could be**. **Risk** depends, among other things, on likelihood and impact. Sometimes the pressing danger isn't an exotic cyberattack, but missing backups, a power failure or too many people sharing one account.

— SO WE'RE NOT BUYING FIREWALL NUMBER THIRTY?

— Not today.

— WHAT IF SOMEONE ATTACKS THE ROOF?!

— Then we'll ask the roofer to perform a vulnerability assessment on the tiles.

A password on a sticky note is wonderfully available

The Manager issued a new rule: every password must have thirty characters, be changed every day and never be written down.

By Monday people were writing them on sticky notes. By Tuesday the notes were under keyboards. By Wednesday reception had a binder labelled “PASSWORDS — DO NOT OPEN”.

— GREG! WHY ARE PEOPLE BREAKING MY RULES?!

— Because you invented a rule that's almost impossible to follow conveniently.

— THEN I BAN INCONVENIENCE!

— Excellent. You're the first man to issue an executive order against reality.

In practice, use **long, unique passwords**, password managers and **multi-factor authentication (MFA)**, while also limiting abusive login attempts and responding to suspected account compromise. Forcing extremely frequent routine password changes without a reason can encourage predictable patterns and unsafe notes. Passwords should not be the only defense. We'll leave the details to a dedicated article on passwords and MFA.

Everyone is an administrator because the Manager trusts people

The tester requested an access-rights report. The accountant could change server settings, the warehouse clerk could delete user accounts and the Manager had full access to everything, despite not knowing what half the buttons did.

— IT BUILDS TRUST! — he explained.

— Who needs permission to delete backups? — asked Greg.

— ANYONE WHO WANTS TO TIDY UP!

— That's like giving every employee keys to the safe, the server room and the cleaning cupboard.

— EXACTLY! ONE KEY, HUGE SAVINGS!

The **principle of least privilege** says that users, programs and services should receive only the access needed for their jobs. Separate duties, use dedicated administrator accounts, remove unnecessary permissions and review access when roles change. That limits the damage from mistakes as well as compromised accounts.

Seven padlocks and an open window

The company had bought a brand-new network firewall. The Manager ordered another antivirus package, a second camera above the entrance and a third security contractor.

— WHY SO MANY LAYERS? — asked Agnes.

— BECAUSE EACH ONE STOPS HACKERS!

— And the warehouse window? — asked Greg.

— WHAT WINDOW?

— The open one. With a sign reading “PLEASE KEEP CLOSED”.

— INSTALL A FOURTH CAMERA IMMEDIATELY!

— Could we close the window first?

Defense in depth uses complementary measures: patching, access control, network segmentation, monitoring, endpoint protection, awareness, backups and incident planning. No single layer offers a hundred-percent guarantee. The layers should address real risks, rather than compete for the largest collection of boxes labelled “SECURITY”.

Patching during the ribbon-cutting

Halfway through the inspection, the building-management system offered an update. The Manager, delighted by a shiny new button, clicked “UPDATE EVERYTHING NOW”. Screens flickered, the printer produced a blank sheet and access control began to reboot.

— GREG! WHAT HAPPENED?!

— You updated the whole system in the middle of the ceremony.

— BUT UPDATES IMPROVE SECURITY!

— Yes. And maintenance windows improve the odds that guests won't have to leave through a window.

Updates fix known faults and vulnerabilities, but critical environments need a plan: assess urgency, test where practical, prepare backups or rollback procedures and understand which components need restarting. Delaying critical patches indefinitely is risky; installing everything without preparation can be risky too.

The backup inside the same burning safe

— AND WHAT IF EVERYTHING STILL FAILS?! — asked the Manager.

— We restore from **backups** — answered Greg.

— WE HAVE THREE COPIES!

— Where?

— IN THREE FOLDERS ON THE SAME DRIVE!

— And if that drive fails?

— MAKE A FOURTH FOLDER!

Agnes glanced at Greg. — Are we going to talk about socks again?

— I'm afraid so.

Security includes **resilience and recovery**. Independent copies, suitable retention, offline backups or backups protected by separate permissions, plus regular restore tests, all help. **RAID** can protect against some hardware failures, but it cannot replace backups. A copy nobody has tested is more of a promise than a plan.

The alarm nobody was allowed to report

Suddenly a monitor displayed an unusual-login alert. The Manager ordered it silenced because it interrupted his speech.

— GREG! TURN OFF THAT ALARM!

— First we need to see what it means.

— WHAT IF IT'S A FALSE ALARM?

— We'll document it and tune the detection rule.

— AND IF IT'S REAL?

— We'll limit access, preserve evidence, assess the scope and recover according to our plan.

— CAN'T WE JUST PRESS “EVERYTHING WILL BE FINE”?

— That button only exists on your desktop.

An incident calls for **detection, assessment, containment, remediation and recovery**. Not every alert means a breach, but ignoring all alerts isn't a strategy. Decide in advance who makes decisions, whom to notify, what to isolate and how to preserve evidence. Afterward, learn from the incident instead of merely looking for someone to blame.

Who watches the Manager?

The inspectors asked for staff training plans and responsibilities. The Manager produced a document titled “SECURITY RULES”. It contained one sentence: “Employees must be careful”.

— What should an employee do with a suspicious email? — asked the inspector.

— BE CAREFUL!

— And if they lose a company phone?

— BE MORE CAREFUL!

— And if someone impersonates you and requests a transfer? — asked Agnes.

— CALL ME!

— Precisely — smiled the accountant. — It might help to write down instructions everyone understands.

Security depends on people, processes and technology. That means clear rules, practice, a culture where mistakes and suspicions can be reported without automatic punishment, and accountability for decisions. Staff don't need to be cryptographers to question a suspicious request. Managers don't have to configure firewalls, but they must understand risk and provide resources.

Finale: a certificate of one hundred percent common sense

After a long day, the inspection team returned to the banner. The Manager looked like a man who had just discovered that no insurance policy covered all of his own ideas.

— SO OUR BUILDING WILL NEVER BE ONE HUNDRED PERCENT SECURE?

— We can't honestly promise that — Greg replied.

— THEN WHAT'S THE POINT OF ALL THESE CONTROLS?!

— To reduce risk, limit damage and keep operating when something goes wrong.

— WHAT DO WE PUT ON THE BANNER NOW?!

Agnes handed him a marker.

— How about “WE THINK, WE CHECK AND WE MAKE BACKUPS”?

— NOT CATCHY ENOUGH!

— But true — said the tester.

The Manager fell silent, then raised his hand triumphantly.

— I'VE GOT IT! “EVERYTHING WILL BE FINE, BECAUSE WE'VE PLANNED WHAT TO DO WHEN IT ISN'T!”

Greg looked at Agnes.

— I admit it. That's the first sensible thing he's said all day.

— PUT THAT IN THE REPORT! — ordered the Manager.

— Already done — replied the accountant. — And backed up.

— WHERE?!

— Not in the same safe.

IT security isn't a promise that nothing bad will ever happen. It's the deliberate protection of what matters, the sensible reduction of risk and the ability to respond when defenses fail. And if someone offers a one-hundred-percent guarantee, ask whether they're also selling concrete for the safe. 🤣

Inspection report: the building may proceed after the defects are corrected. The “100% GUARANTEED” banner has been sent to Marketing. Greg got his sandwich back. His annual leave remains missing. 🤣❤️