Lepší je být připraven, než překvapen

Patrik Matejsek

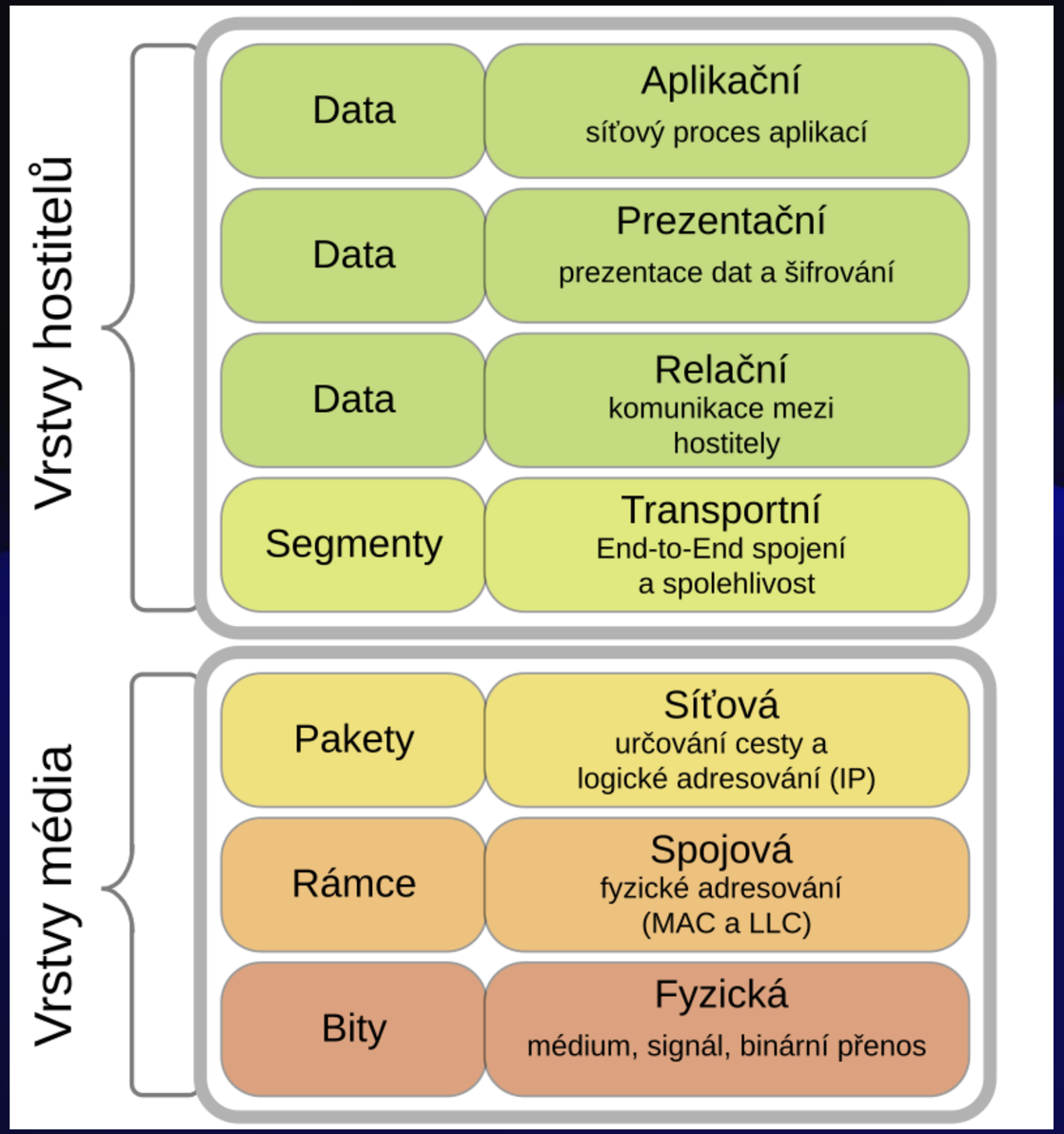
TAKTIK

„V ČR dochází denně k desítkám tisíc pokusů o kybernetický útok každý den…“

Odhady se mohou lišit, ale v každém případě je kybernetická bezpečnost v ČR stále velmi aktuálním tématem a útočníci jsou velmi aktivní.

Jak vlastně digitálně komunikujeme?

Referenční model ISO/OSI a jeho návaznost na reálné vektory útoku.



Co znamená být připraven?

„Neznamená to mít plán na papíře. Je to o jasné strategii reakce na krizové situace."

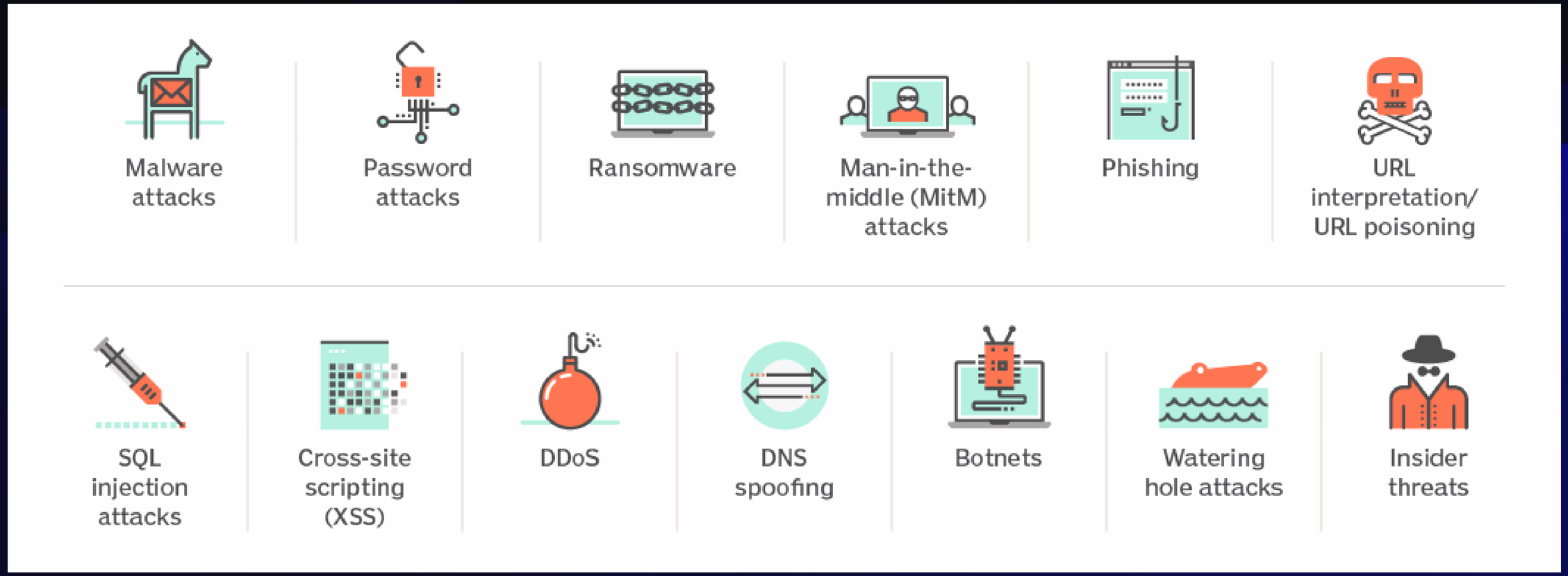
- Předcházení problémům.
- Nebát se investic do bezpečnosti.
- Vytvoření krizového plánu.
- Sledování aktuálních hrozeb.
- Vlastnit prostředky a nástroje pro zvládnutí vzniklé situace.

„Auto byste neukradli. Peněženku byste neukradli. Televizi byste neukradli…“

A přesto tento spot občas běžel i na čerstvě vypálených digitálních médiích…

Typy útoků a nečekaných situací

Vycházíme ze znalosti síťového prostředí a známých metod kybernetických útoků dle jednotlivých možností.



Typy útoků a nečekaných situací

Vycházíme ze znalosti síťového prostředí a známých metod kybernetických útoků dle jednotlivých možností.

- Zasahuje veškeré vrstvy síťového modelu.
- Nevyhneme se fyzické bezpečnosti.
- Sonda do vlastní počítačové sítě jako základ.
- Firewall nerovná se čistě transportní vrstva.
- Silné heslo je dlouhé heslo?
- Kontrola dodavatelského řetězce.
- SIEM jako dogma

Je možné být více proaktivní?

Klíčem je Threat Intelligence…! Aneb není nad to připravit se na neznámé hrozby dříve, než nastanou.

- Proces sběru, analýzy a využívání informací o hrozbách.
- Dlouhodobé analýzy a globální trendy.
- Konkrétní techniky a nástroje, které útočníci používají.
- Ochrana vlastní značky.
- Dark web bez loupání…

"Pokud víme, že útočníci zneužívají konkrétní zranitelnost v historicky zneužité společnosti, můžeme nasadit opravy a záplaty předtím, než bude útok realizován.“

Případně nabité znalosti použít pro následné vyjednávání…

Možnosti další integrace

Když se nástroj spojí s nástroji a vznikne mocný prostředek.

- SIEM na steroidech.
- XDR jako základ autonomního SOC.
- Kontejnery nevyvážejí pouze popeláři.
- Šifra mistra Leonarda, ale vaše, milé HSM…

„Protože u Magdy, co umí bezva kafe, to začalo…“

Ale také skončilo, protože Magda ví…ale někde možná ani neví.

100 %

ochrana neexistuje, ale děláme pro ni maximum…

Děkuji za pozornost.

Prostor pro možné dotazy…