Digitalk

REPORT

Индустриална киберсигурност

Индустриална киберсигурност

#4

Индустриалната киберсигурност – как да не влезем в новините

#13

Слабото звено в индустрията води до огромни проблеми

#26

Зловредният код и човешките грешки допринасят за пандемията от рансъмуер

#34

Производствената индустрия под квантова заплаха

ИНДУСТРИАЛНАТА КИБЕРСИГУРНОСТ – КАК ДА НЕ ВЛЕЗЕМ В НОВИНИТЕ

Александър Главчев

В средата на октомври сайтовете на български институции станаха обект на DDoS атака. Според главния прокурор Борислав Сарафов тя е била стартирана от град Магнитогорск в Руската федерация. Хакерска група, нарекла себе си We are killnet, обяви, че кампанията е заради „предателството на България към Русия и доставки на оръжие за Украйна“. Това е реалността днес, като трябва да се подчертае, че нещата не започнаха с войната, разразила се само на няколкостотин километра от границата ни.

През 2019 г. се случи вероятно най-големият теч на лични данни в България. Хакерска атака срещу Националната агенция за приходите доведе до публично разпространяване на архив с информация за милиони българи. Големи и малки организации са изправени пред все по-сложни киберзаплахи. Независимо дали става въпрос за стартираща компания със

свързан продукт или утвърдена корпорация с дългогодишен опит в областта, в момента е по-важно от всякога да се осъзнават реалностите и тенденциите в сферата на киберсигурността. България не е изключение - в началото на октомври, по време на старта на Европейския месец на киберсигурността, Министерството на електронното управление излезе с данни, че 57% от организациите у нас са подложени на ежеседмични фишинг атаки.

Организациите са изправени пред увеличаване на броя на атаките и пробивите в сигурността, като се очаква тенденцията да се запази следващите години. По данни на IBM разходите вследствие на пробиви с изтичания на данни през 2021 г. възлизат средно на 4.24 млн. долара за един случай. За да избегнат такива големи разходи, предпри-

ятията трябва да разполагат с подходяща инфраструктура за предотвратяване поне на най-широко разпространените заплахи.

НАТИСК ОТГОРЕ

В отговор на увеличаващите се като брой и мащаб заплахи ръководствата на организациите все повече ще назначават директори с ресор именно информационната сигурност - CISO (Chief information security officer). Постепенно през последните няколко години, с увеличаващите се случаи на пробиви, течове, откупи и солени глоби, се забелязва значително повишаване на информираността за заплахите сред висшите ръководители.

Допълнително, бидейки част от мениджмънта, CISO все по-често ще докладват директно на главния изпълнителен директор, финансовия директор или на борда на компанията. Следователно хората на тези позиции ще трябва не просто да познават добре своя ресор, но и да владеят други нетехнически умения, благодарение на които да могат да представят на нетехническото висше ръководство стратегиите за киберсигурност на организацията.

Също CISO трябва да разполагат и широк поглед върху цялата организация - да са наясно рисковете и уязвимостите, но и за това кои са критичните процеси. Според доклад на Gartner от 2021 г. през 2025 г. 40% от бордовете на директорите ще имат специален комитет по киберсигурност, контролиран от член на борда. За сравнение - днес (т.е. през 2021 г.) тези компании са по-малко от 10%.

ОСНОВНИ ТЕНДЕНЦИИ ПРИ КИБЕРСИГУРНОСТТА ПРЕЗ 2023 Г.

ДИСТАНЦИОННА РАБОТА

Въпреки че работата от вкъщи или просто извън офиса съществуваше и преди пандемията, масовото възприемането на този модел се случи последните две години. Компаниите се стремяха да продължат с нормалните бизнес операции въпреки строгите ограничения по време на пандемията.

„Новото нормално“ обаче не дойде без нова порция трудности. Киберпрестъпниците насочват вниманието си към отдалечените работници, които, намирайки се извън пределите на офисните мрежи, в много случаи се оказват по-уязвими. Занапред дистанционната работа ще продължи да доминира, както и свързаните с нея заплахи. Сред тях са фишинг атаките, уязвимите пароли, незащитените домашни устройства и др.

РАНСЪМУЕР АТАКИ

Рансъмуерът продължава да е най-значителният риск от гледна точка на киберсигурността за компаниите и през 2022 г., като тази тенденция вероятно ще продължи. Подобно на атаките срещу отдалечените работещи, кампаниите с криптовируси се възползваха от хаоса по време на пандемията и продължават да предизвикват значителни главоболия, особено в сектори като този на здравеопазването.

У нас нашумял случай в тази посока бе криптирането на

данни на „Български пощи“, за което на държавната структура бе наложена санкция в размер на 1 млн. лв. от Комисията за защита на личните данни (КЗЛД). Актът бе за това, че дружеството „не е приложило подходящи технически и организационни мерки“ преди и по време на кибератаката.

ВЕРИГИ ЗА ДОСТАВКИ

Киберпрестъпниците продължават да използват по-модерни и усъвършенствани техники, за да се насочват към отдалечени работници, и част от вниманието им е насочено към веригите за доставки (supply chain).

Станалият вече знаменит пробив в сигурността на SolarWinds от 2020 г., когато хакери успяха да проникнат в мрежите на компанията и тайно да променят кода в един от пакетите за актуализация на нейния софтуер, излагайки на риск хиляди организации, използващи нейния продукт, продължава да е показателен пример.

ОБЛАЧНИ РИСКОВЕ

Облачните изчисления са една от най-революционните технологии, на които станахме свидетели през последното десетилетие. Данните са ключов актив за всяко предприятие и затова не е учудващ повишеният интерес на киберпрестъпниците към облачните хранилища и услуги.

Неправилно конфигурираната облачна изчислителна инфраструктура е една от основните причини за заплахи в тази посока. Други възможни причини са проблемите с миграцията, вътрешните рискове, хакване на акаунти и

несигурните интерфейси. С увеличеното възприемане на частни, публични и смесени облачни модели и все по-големите количества данни, съхранявани в тези инсталации, не е трудно да се предвиди, че заплахите в тази насока ще се увеличават през 2023 г. и занапред.

КЪДЕ ДА СЕ ИНВЕСТИРА ПРЕЗ 2023 Г.

Три са основните фактори, влияещи върху разходите за киберсигурност, считат анализаторите от Gartner. Това са ръстът при дистанционната и хибридната работа, преходът от виртуални частни мрежи (VPN) към мрежов достъп с нулево доверие (ZTNA), както и преминаването към облачни модели за доставка.

От Gartner очакват, че разходите за информационна сигурност и продукти и услуги за управление на риска ще нараснат с 11.3%, за да достигнат повече от 188.3 млрд. долара през 2023 г. Сигурността в облака е категорията, за която се прогнозира най-силен растеж през следващите две години. С увеличения фокус организациите върху ESG, риска от трети страни, риска по отношение на киберсигурността и риска за поверителността Gartner прогнозира, че пазарът на интегрирано управление на риска (IRM) ще демонстрира двуцифрен растеж до 2024 г., като по-голямата конкуренция доведе до по-евтини решения.

Услугите за сигурност, включително консултациите, хардуерната поддръжка, внедряването и външните услуги, са най-голямата категория разходи с почти 72 млрд. долара през 2022 г. и се очаква да достигнат 76.5 млрд. долара през 2023 г.

ДИСТАНЦИОННАТА РАБОТА ВСЕ ОЩЕ СТИМУЛИРА ИНВЕСТИЦИИ

Търсенето на технологии, които позволяват сигурна дистанционна и хибридна работна среда, ще се увеличи след 2022 г., предвиждат още анализаторите. Докато организациите се стремят да създадат сигурна среда за работа от вкъщи, те проучват решения, които предлагат бърза възвръщаемост на инвестициите. В резултат на това технологии като защитни стени за уеб приложения, управление на достъпа, платформа за защита на крайни точки (endpoint protection platform, EPP) и защитен уеб портал (secure web gateway, SWG) ще бъдат свидетели на поне краткосрочно търсене.

МРЕЖОВИ ДОСТЪП С НУЛЕВО ДОВЕРИЕ

ZTNA (Zero Trust Network Access) е най-бързо развиващият се сегмент в мрежовата сигурност, като се очаква да нарасне с 36% през 2022 г. и с 31% през 2023 г., отново воден от търсенето на възможности за защита на отдалечени служители и намаляване на зависимостта на организациите от VPN. С увеличаването на информираността по отношение на ZTNA подходът ще се използва не само при отдалечена работа, но и за служители в офисите. Gartner прогнозира, че до 2025 г. най-малко 70% от новите внедрявания не решения за отдалечен достъп ще бъдат обслужвани предимно от ZTNA вместо от VPN услуги спрямо по-малко от 10-те на сто в края на 2021 г.

ОБЛАЧНИ МОДЕЛИ ЗА ДОСТАВКИ

Заради използването на многооблачни среди организациите са изправени пред повишени рискове за сигурността, както и увеличена сложност при управлението на множество технологии. Това ще доведе до тласък към облачна сигурност и пазарният дял на облачните решения ще нарасне.

Според анализаторите комбинираният пазар за брокери за сигурност на достъпа до облака (Cloud Access Security Brokers, CASB) и платформи за защита на работното натоварване в облака (Cloud Workload Protection Platform, CWPP) ще нарасне с 26.8%, за да достигне 6.7 млрд. долара през 2023 г. Търсенето на облачни решения за откриване и реагиране на опасности - като например в крайни точка (Endpoint Detection and Response, EDR), или т.нар. решения за управлявано откриване и реагиране (Managed Detection and Response, MDR) - също ще се увеличи през следващите години.

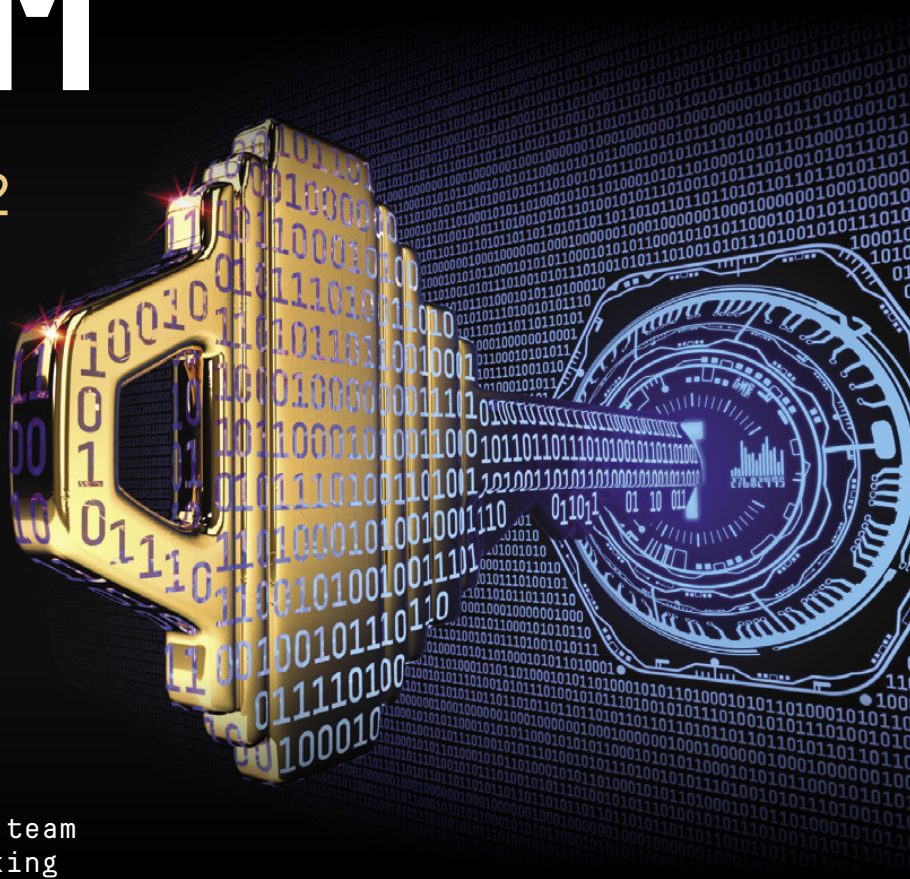
КАПИТАЛ

STRATEGIC PARTNER: amatas

CYBER SECURITY FORUM

17 November 2022

Onsite and Online



The Cybersecurity conference's team from Capital and ATAMAS is looking forward to hearing your ideas!

Open call for more speakers!
For more details, please see the website

SAVE THE DATE
capital.bg/cyber2022

General partners

VIVACOM · pwc · KPMG · INFORMATION SERVICES

Main partners

nexo · Hewlett Packard Enterprise operated by Selectium · telelink BUSINESS SERVICES · ESCOM Enterprise ICT Security Solutions · mastercard · vmware · NDB · IBM · DIGITALL

NETERRA telecommunications · Acronis

СЛАБОТО ЗВЕНО В ИНДУСТРИЯТА ВОДИ ДО ОГРОМНИ ПРОБЛЕМИ

Владимир Владков

Shutterstock

Сигурността е комплексна многопластова област, която засяга много понятия: от защита на данни и доверие в тях до устойчивост на процесите. В днешните свързани общества сигурността трябва да проникне във всички аспекти на съвременните технологии, за да поддържа успешни цифрови и киберекосистеми. Слабото звено във веригата може да представлява отворена врата за заплаха или да бъде излагане на риск заради неправилно конфигуриране.

Всяка връзка, всеки слой трябва да бъдат защитени. И все пак начинът, по който сигурността се внедрява досега, варира изключително много, повлиян е от различни фактори: цена, регулиране, технологични ограничения, пазарно търсене. Всички те влияят в различна степен върху инвестициите в сигурността. Най-големите предизвикателства за по-бързо внедряване на сигурността се крият в разбирането за добавената стойност на технологията, след това следва намирането на правилното решение, което да бъде приложено по ефективен начин. Единодушно е мнението обаче, че сигурността е необходима - но къде и как, кога и до каква степен е доста трудно да се определи.

Например защо идентичността е важна за свързаните обекти? Какви атрибути на избраното хардуерно решение за сигурност могат да бъдат най-ефективно интегрирани в инфраструктура с публичен ключ? Кои вертикални сектори ще бъдат засегнати както в краткосрочен, така и в дългосрочен план? Какви приложения ще бъдат приоритетни и на каква цена?

БЕЗПРЕЦЕДЕНТНА ПРОМЯНА

Пандемията COVID-19 се оказа промяна за мнозина. Не всички, но повечето индустриални предприятия бяха „ужасно“ неподготвени, коментира Джонатан Гордън, анализатор от TP Research. През първите дни на пандемията много инженерни и оперативни екипи бяха буквално изолирани на място във фабриките - ситуация, която не можеше да продължава дълго. Непосредствената нужда за много предприятия бе да разберат как да свържат дистанционно всеки, който се нуждае от достъп до тези мрежи и устройства. „За съжаление необходимостта от бърза реак-

ция често води до отваряне на нови дупки в сигурността, вместо да се затварят - добавя Гордън. - Днес много от нас все още се занимават с тези проблеми."

Пандемията COVID-19 доведе до оперативни промени в промишлените предприятия, тъй като набързо изградените краткосрочни решения се превърнаха в дългосрочно статукво за много бизнеси. Освен други фактори пандемията повлия и върху организационния подход към киберсигурността и управлението на рисковете.

Някои от промените, предизвикани от пандемията, са положителни и необходими, други не толкова, допълва анализаторът от TP Research. Въпреки че първоначално забави инициативите, отговорът на пандемията създаде катализатор, който съживи проектите за сигурност. В крайна сметка нуждите и решенията за киберсигурност ще разтърсят пазара.

Войната в Украйна значително повиши нивата на тревога и активните действия за защита на критичната и друга инфраструктура от киберзаплахи. „Ако не друго, това демонстрира колко преплетени са световните икономики и колко податливи са глобалните вериги за доставки както на физически, така и на киберзаплахи - коментира Гордън. - В личен план използвам възможността да заявя, че безсмисленото и брутално нахлуване в Украйна беше напълно опустошително за всички. Мислите ми са постоянно с колеги и приятели, страдащи от войната и живеещи под окупация", допълва той.

Според него през последните една-две години сме свидетели на „безмилостни" кибератаки срещу всякакви кри-

тични инфраструктури - от ВиК, през газопроводи до транспортни системи. Colonial, Oldsmar, JBS, Molson Coors, NHS, гръцкият оператор на газопроводи DESFA, британската компания за обществен транспорт Go-Ahead - списъкът на жертвите в ключови вертикали продължава да расте. „Ако нещо е ясно в този момент, то е, че собствениците на активи и операторите са изправени пред непосредствена пряка опасност“, добавя той.

И цифровата, и киберсигурността трябва да останат адаптивни към предизвикателна и сложна реалност, коментират и от ABI Research. Това важи с особена сила днес, когато върху компаниите и пазарите влияят фактори като бързия темп на технологична еволюция и дигитална трансформация чрез облачна миграция, разширяване обхвата и възможностите на IoT, ускореното внедряване на 5G мрежи и услуги, напредъка в областта на изкуствения интелект (AI), подобрените възможности на периферните (Edge) изчисления и нарастваща автоматизация. Анализаторите от ABI Research представят няколко ключови тенденции в тези сектори, давайки и прогнози за развитието на технологичните решения в областта на индустриалната киберсигурност:

РАЗШИРЯВАЩАТА СЕ ЕКОСИСТЕМА ОТ РЕШЕНИЯ ЗА ЗАЩИТА НА ВЕРИГАТА ЗА ДОСТАВКИ

Докато технологиите за по-добра видимост на активите на предприятието и тяхната защита стават все по-зрели за индустриалните оператори, сигурността на оперативните технологии (OT) във веригата за доставки все още е в зародиш. Управлението на риска при трети

страни и управлението на веригата за доставки са нововъзникващи дисциплини, с нови решения, фокусирани върху надлежната проверка, редовни одити, планове за гарантиране на сигурността, цялостна актуализация на фърмуера „по въздуха“ (FOTA) и управление на достъпа за доставчиците на услуги. До голяма степен тези концепции са пряко свързани с подобряването на цялостната киберустойчивост на индустриалните оператори и са неразделна част от управлението на жизнения цикъл на активи, мрежи и операции, което идва с интеграцията на Industry 4.0.

ПОДГОТОВКА НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ ЗА АКТИВНИ КИБЕРРЕШЕНИЯ

Индустриалните предприятия включват все повече революционни технологии при своята миграция към Индустрия 4.0 Това стимулира по-доброто оценяване на изискванията за киберсигурност на киберфизичните системи, индустриалния Интернет на нещата (IIoT), интелигентното производство, адитивното производство и редица други. Търсенето на тези технологии има допълнителен ефект върху индустриите, класифицирани като критична инфраструктура, при които преходът към Индустрия 4.0 е по-бавен, а киберсигурността продължава да разчита на традиционни набори от инструменти за сигурност на информационните технологии (ИТ) за защита на оперативните технологии ОТ (т.е. управление на отдалечен достъп, инвентаризация на ОТ активи, индустриални защитни стени и др.). Въпреки това появата на изкуствен интелект (AI) и машинно обучение (ML), автоматизация и оркестрация за активиране на нови приложения за сигурност като бързо превключване на потребители, корекции

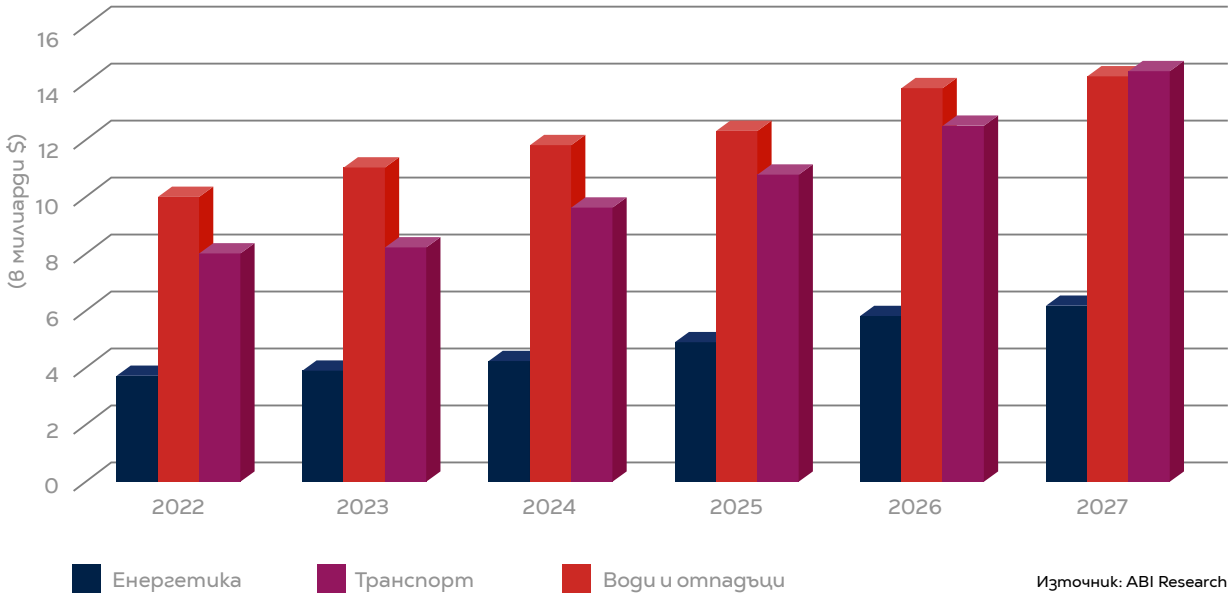
в работен режим без спиране, облачно базирана система за индустриален контрол (ICS), мрежови сонди и програмиране на защитен програмируем логически контролер (PLC) бавно, но сигурно привлича операторите на критична инфраструктура.

Доставчиците на OT киберсигурност трябва да гарантират, че имат диференцирани продуктови решения и предложения за услуги за различните критични инфраструктури, тъй като те подлежат на и спазват различни регулаторни и стандартни изисквания. Освен това те са на различен етап от възприемане на Индустрия 4.0 и следователно приоритетът на защитата на наследените спрямо интелигентните активи може да варира значително. В секторите с по-бавен преход доставчиците трябва да имат по-специализирани познания по отношение на системите за контрол, с които разполага фабриката, докато в индустрии с по-интелигентна инфраструктура фокусът трябва да бъде върху новите възможности, предлагани от сигурни микроконтролери (например доверени, т.е. надеждни среди за изпълнение) или защитни механизми, присъщи на 5G мрежите (например взаимно удостоверяване).

Очаква се глобалните разходи за киберсигурност в критичните индустриални инфраструктурни сектори (енергетика, транспорт и управление на водите и отпадъците) да достигнат $23 милиарда до края на 2022 г., като ще нараснат през прогнозния период с 10% CAGR (виж графиката) . Въпреки че транспортният сектор е най-напреднал по отношение на интегрирането и внедряването на инструменти за киберсигурност, пандемията намали бюджетите и инвестициите в сектора, коментират от ABI Research.

Най-засегнатият в бъдеще обаче ще бъде енергийният сектор. Настоящата война на Русия срещу Украйна принуждава западните страни да се откажат от петрола и газа и да ускорят прехода към по-устойчива енергия. Този план беше в техните програми за влияние върху изменението на климата, макар и в много по-дълъг период от време. Това ще окаже пряко въздействие върху киберсигурността както при петрола и газа, първоначално в контекста на войната, така и занапред при осигуряването на енергийния преход и новите начини на производство на електроенергия, добавят анализаторите.

РАЗХОДИ ЗА СИГУРНОСТ НА КРИТИЧНА ИНДУСТРИАЛНА ИНФРАСТРУКТУРА, ПО СЕКТОРИ



Източник: ABI Research

ОПТИМИЗИРАНА ЗАЩИТА НА ДАННИТЕ ОТ ТЕЛЕМАТИКАТА

Защитеното управление на данни от автомобилни телематични приложения става все по-важно за производите-

лите на превозни средства, доставчиците на части, телекомите и застрахователните компании. Почти всеки аспект на софтуерно дефинираното превозно средство е настроен да включва постоянно развиващи се технологии за киберсигурност на хардуерно, софтуерно и мрежово ниво, като сигурността на телематичните данни е една от основните операции. Стремежът да се увеличи надеждността на телематичните данни, да се разбере как те могат да бъдат „осребрени“ по-добре и да се създаде възможност за интелигентно управление на автономни превозни средства подхранва дигитализацията на превозните средства, управлението на автопарка и приложенията автомобил към всичко останало (Vehicle-to-Everyt hing - V2X). На пазара на решения за телематична сигурност това се отразява чрез постоянната еволюция на телематичните контролни устройства (TCU) и мрежовите функции, които те задействат.

Услугите за сигурно управление на данни в свързаната телематика на превозните средства са жизненоважни за по-нататъшното усъвършенстване на разузнавателните операции и отключването на V2X хоризонта за виртуалните машини. Доставчиците на услуги за сигурност трябва внимателно да се съгласуват с целите на виртуалните машини относно функционалната безопасност и физическата сигурност. Това може да даде възможност за нови потоци за монетизиране на сигурността на IoT в свързаните превозни средства чрез предлагане управление на идентичността и на достъпа и сигурни комуникации. Доставчиците на облачна сигурност трябва да разработят оптимизирани за сигурността платформи за управление на автомобилния парк, предлагайки различни нива на управление на жизнения цикъл на устройство-

то въз основа на идентификационни данни за криптиране, налични в TCU. За приложения от по-високо ниво това може да се разшири до разработването на по-сложни центрове за сигурност (SOC), специфични за превозните средства. Доставчиците на вграден хардуер могат да помогнат за оформянето на пазара чрез разработване на уникални стойностни предложения около вградени модули за самоличност на абоната (eSIM), модули за надеждна платформа (TPM) и хардуерни модули за сигурност (HSM), като адаптират своите продукти към бъдещи нужди от свързаност, базирани на събиране на данни (например скорост, местоположение, пробег и т.н.) за справяне с управлението на данни в превозното средство и за осигуряване на актуализации на фърмуера по въздуха (FOTA) за TCU.

ЗАЩИТА НА УМНИТЕ ЕЛЕКТРОМЕРИ

Нарастващото внедряване на интелигентни електромери в световен мащаб, дължащо се на прехода към усъвършенствана измервателна инфраструктура (AMI), увеличава изискванията за сигурно управление на идентичността на устройствата и нуждата от интелигентни измервателни уреди, работещи в мобилни клетъчни и нискоенергийни широкообхватни мрежи (LPWA) от типа на LoRa и NB-IoT. Доставчиците на облачни услуги могат да предложат ценни решения за киберсигурност на доставчиците на комунални услуги за техните интелигентни измервателни уреди, включително широк набор от цифрови сертификати и опции за управление на жизнения цикъл на устройствата като услуги на сертифициращи органи (CA) и инфраструктура с публичен ключ (PKI).

ЗАКОНОДАТЕЛИ И РЕГУЛАТОРИ СА „ЗАПРЕТНАЛИ РЪКАВИ“

Глобалните вериги за доставки са изправени пред сериозни заплахи от национални държави и престъпни хакери, които се стремят да откраднат чувствителна информация и интелектуална собственост, да компрометират целостта на правителствени системи, предприемат и други действия, които оказват неблагоприятно въздействие върху способността на държавните организации да предоставят на своите граждани услуги безопасно и надеждно.

„Въпреки че това е доста мрачна картина, има някои положителни страни и по-специално, разговорите за индустриалната киберсигурност стават по-професионални“, коментира Гордън. „Освен това има реакция от всички участници - от индустрията, от правителствата, от индустриалните асоциации, които работят за изграждане и укрепване на организационната позиция на киберсигурността“, добавя той.

Правителствата по света вече започнаха да действат. Например заповедта на президента на САЩ предизвика бурна активност, макар и все още недобре насочена. Тя помогна да се подчертаят опасенията за киберсигурността, които тормозят индустрията. Директивата TSA е един такъв пример.

Сингапур също актуализира своя „Практически кодекс за киберсигурност за критична информационна инфраструктура“, който влезе в сила през юни тази година, допълва Гордън. Австралийското правителство прие законопроект за защита на критичната инфраструктура, като целта е да се повишат сигурността и устойчивостта на рамката на

критичната национална инфраструктура, защита на основните услуги, на които австралийските граждани разчитат, от физически заплахи, заплахи по веригата на доставки, киберзаплахи и заплахи от страна на персонала.

По същия начин Федералната агенция на САЩ CISA разработва разпоредби след Закона за докладване на киберинциденти за критична инфраструктура, който беше подписан от президента на САЩ Джо Байдън през март.

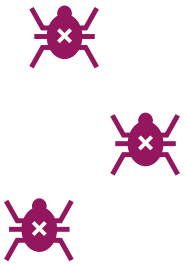
Директивата NIS2 на Европейския съюз се допълва от редица правителствени и специфични за индустрията разпоредби и работни рамки - стандартите IEC 62443, ръководството NIST 800-82, рамката MITER ATT&CK и други.

КАКВО ПРЕДСТОИ?

Киберрискът по същество е бизнес риск. За да смекчим тези рискове, имаме нужда от инструменти и процеси, които да ви позволят да видите и разберете текущата картина, да промените тази картина и да повлияете върху резултата, казва Гордън.

Доскоро доставчиците на решения се фокусираха върху осигуряването на видимост и инвентаризация на активите. Въпреки че много индустриални предприятия са внедрили решения, включително инструменти за видимост и инвентаризация на активи, много други все още не са го направили. „Като индустрия трябва да започнем да гледаме на защитата на индустриалните предприятия от край до край. Да идентифицираме и сегментираме критични за бизнеса процеси, да измерваме риска и да прилагаме поне базова киберхигиена“, добавя анализаторът.

ИНДУСТРИАЛНА КИБЕРСИГУРНОСТ



КИБЕРФИЗИЧНА СИГУРНОСТ И ПРЕДПАЗВАНЕ НА ОПЕРАТИВНИ СИСТЕМИ

- Интегритет на OT устройства & сигнали
- Манипулиране на данни
- Прогнозна поддръжка

УПРАВЛЕНИЕ НА ИДЕНТИЧНОСТТА И ДОСТЪПА (IAM)

- IAM - управление на правила и роли
- Управление на идентичността (ID)
- MFA, SSO & PAM

СИГУРНОСТ НА ИНДУСТРИАЛНИ IOT (IIOT) УСТРОЙСТВА

- Вграден IoT агент
- Инвентаризация на IIoT - хардуерни/ софтуерни
- Управление на постоянна уязвимост
- Валидиране на актуалната защита на устройствата

СИГУРНОСТ НА IT/OT КРАЙНИ ТОЧКИ И УПРАВЛЕНИЕ НА „КРЪПКИТЕ“

- Защита на индустриални IT крайни устройства (HMI (интерфейси човек/ машина), работни станции и др.)
- Крайните OT точки (DCS (разпределени контролни системи), PLC (програмируеми логически контролери), RTU (отдалечени терминали) и други)
- Управление на конфигурирането

МОНИТОРИНГ НА МРЕЖИТЕ И ЗАСИЧАНЕ НА ЗАПЛАХИТЕ

- Засичане на аномалии и заплахи в мрежата
- Откриване и „картографиране“ на мрежови активи
- Автоматизирана инвентаризация на мрежата
- Мониторинг, предупреждения и доклади

ПЕРИМЕТРОВА СИГУРНОСТ И СЕГМЕНТИРАНЕ НА МРЕЖАТА

- Шлюзове за данни
- Индустриални защитни стени (Firewall)
- „Дезинфекция“ на USB медии

УПРАВЛЕНИЕ НА РИСКА И РЕГУЛАТОРНИ СЪОТВЕТСТВИЯ

- Анализ на състоянието и доколко системите са изложени на рискове
- Управление на риска
- Намаление на рисковете и приоритизация на уязвимостите
- Разузнаване за актуални заплахи

ЗАЩИТЕН ОТДАЛЕЧЕН ДОСТЪП

- Мултивендорна платформа за отдалечен достъп
- Контрол на достъпа и дневник на влизанията
- Отдалечен достъп с „нулево“ доверие VPN достъп.

Sophisticated threats, meet modern security

Legacy endpoint security tools are no longer enough. Stop these evolving threats with the modern endpoint security solution **VMware Carbon Black Cloud ™.**

NDB | VMware distributor and Authorized Training Center for Bulgaria **| ndb.bg**

Q&A

Ива Ташева,
съосновател на CYEN

ЗЛОВРЕДНИЯТ КОД И ЧОВЕШКИТЕ ГРЕШКИ ДОПРИНАСЯТ ЗА ПАНДЕМИЯТА ОТ РАНСЪМУЕР

Q&A

***Ива Ташева** е съосновател на базираната в Белгия консултантска компания CYEN. Тя е член на групите по информационна сигурност и облачна сигурност на Агенцията на Европейския съюз за киберсигурност (ENISA) и основател на белгийската камара Women4Cyber. Тя е и един от десетте финалисти в конкурса „Личност на годината“ за 2022 година, организиран от белгийската „Коалиция по киберсигурност“.*

Вие сте сред финалистите на белгийския конкурс „Личност на годината в областта на киберсигурността“. Разкажете малко повече за конкурса и как попаднахте там.

Конкурсът се организира за втора поредна година от белгийската „Коалиция за киберсигурност“. Инициативата цели да насочи вниманието върху талантите в сферата на киберсигурността в Белгия. Аз бях номинирана заради активното ми участие в инициативите за подобрение на киберсигурността на европейско ниво, а също и по повод на лансирането на инициативата „Жените за киберсигурността в Белгия“ (Women4Cyber Belgium chapter), на която съм съучредител.

Какво е за вас тази номинация?

Тази номинация преди всичко означава, че европейските инициативи за киберсигурност, в които участвам, са от значение и се ценят в страните членки, включително в Белгия. В личен план това е огромно признание за работата и приноса ми към киберсигурността.

Q&A

А какво е да си жена, която работи в областта на киберсигурността?

Доскоро бе самотно. През 2022 г. едва 25% от професионалистите в киберсигурността са жени, макар и този дял да расте. Случвало ми се е да съм единствената жена, единственият чужденец и единственият човек под 35 години в екип от 10 души. За мен това е отговорност да проправя път и за другите. Такава е и целта на новата инициатива в Белгия „Жените за киберсигурността“. Като част от нея вече създаваме групи по интереси и ще работим, за да подобрим условията и участието на жените в сектора.

Говорим за киберсигурност, какви са последните тенденции при атаките и съответно при методите за защита?

Основните проблеми остават зловредният код и човешките грешки. Тези два фактора допринасят за пандемията от рансъмуер. Чрез заблуждаване на потребителя и подтикването му да въведе данни или да отвори заразен файл или линк нападателят може да поеме контрол над данните и системите на организацията и да изиска откуп от легитимния собственик за възстановяване на достъпа. Най-лесните мерки за предпазване от този тип атака включват предпазливост към съобщения от непознати податели и поддържане на последната версия на системите, включително антивирусен софтуер. Може да използвате сигурна връзка (VPN) за корпоративните системи и данни, за да намалите риска, свързан с несигурната Wi-Fi връзка.

Q&A

Човешкият фактор продължава да е препъникамъкът на сигурността, въпреки че вече говорим за човешка защитна стена. Ще стигнем ли до момента, в който няма да говорим толкова често за човешки грешки?

С автоматизацията на процесите в организацията мисля, че в бъдеще трябва да говорим повече за добрите примери и иноваторите в киберсигурността, отколкото за човешките грешки.

Темата за киберсигурността все по-често е във фокуса на управлението на компаниите (а не само в полезрението на мениджърите по информационна сигурност). Означава ли това, че бизнесът си е научил урока?

По време на масовата дигитална трансформация, която се ускори вследствие на рестрикциите, свързани с ковид пандемията, стана ясно, че сигурността на данните и системите играе ключова роля за сигурността на бизнеса. До този момент бе трудно да определим какво е отражението на киберсигурността върху бизнеса, тъй като често можеше да продължим бизнес услугите си без наличието на дигитални системи. Дотогава говорехме само за глоби, свързани с GDPR, ако лични данни са изтекли поради лип-

> *„Да си жена в киберсигурността е самотно. През 2022 г. едва 25% от професионалистите в областта са жени.“*

Q&A

са на адекватни мерки за киберсигурност. Това вече не е така. Бизнесът не може без конфиденциалност на личните данни, както и без достъп до надеждни системи и информация.

Често говорим за превенция, но за целта трябва да има споделяне на информация между заинтересованите страни (нещо, което малко компании са склонни да направят). Как бизнесът може да бъде научен да споделя, че е бил обект на атаки?

Бизнесът трябва да намери полза и да се чувства в сигурна среда, за да споделя чувствителна информация относно киберинциденти. Първата стъпка може да бъде споделяне на информация в секторни групи, като така получената информация ще има най-голяма полза поради спецификата и релевантността ѝ за сектора (общи системи, процеси и доставчици). За да се създаде сигурна среда за споделяне, бизнесът трябва да научи каква информация, колко и кога да разкрива. Необходимо е да има сигурни канали за споделяне между заинтересованите страни при евентуални атаки, като невинаги информацията трябва да става обществено достояние. Най-накрая, да не забравяме, че GDPR въведе задължение за известяване при нарушаване на сигурността на личните данни. Критичните сектори (като енергетика, транспорт, финансови услуги) вече са задължени да известяват компетентните органи за осъществени атаки според Директива на ЕС за мрежова и информационна сигурност (NIS Directive).

Да поговорим за законодателството. Адекватно ли е то в момента на проблемите на киберсигурността?

Q&A

„С автоматизацията на процесите в организацията мисля, че в бъдеще трябва да говорим повече за добрите примери и иноваторите в киберсигурността, отколкото за човешките грешки.“

Актуалното законодателство, основно на европейско ниво, покрива абсолютния минимум и е лимитирано в обхват (финансови услуги, критична инфраструктура, медицински изделия). В момента се разработват три основни директиви, които ще допълнят това законодателство, покривайки киберсигурността на свързаните продукти и на производителите на продукти с дигитални елементи (например за обмен на информация) и изкуствения интелект. Но, както винаги, заплахите за киберсигурността се движат със скоростта на светлината, образно казано, докато при законодателството са нужни 5-7 години от инициативата до въвеждането му. Това е сериозно предизвикателство за адекватността му.

Каква трябва да бъде ролята на държавата в тази екосистема?

Както при физическата сигурност на гражданите, държавата трябва да предоставя инфраструктурата, правилата и институциите за киберсигурност. Нейна е ролята и да гарантира сигурни обществени услуги. Тя трябва да насърчава бизнеса чрез инвестиции в киберсигурността и развитие на учебни програми, за да спомогне за намаля-

ването на дефицита на умения.

А каква е ролята на мениджъра по информационна сигурност (CISO) в изграждането на адекватна защита и превенция и какво трябва да е неговото място в корпоративната общност?

Според новата рамка за умения в областта на киберсигурността на Агенцията на Европейския съюз за киберсигурност (ENISA) CISO управлява стратегията на организацията в тази област и нейното прилагане, за да гарантира, че цифровите системи, услуги и активи са достатъчно сигурни и защитени. Мениджърът по информационна сигурност би трябвало да подкрепя бизнес лидерите при вземане на стратегически и операционни решения с цел осъществяване на мисията на организацията и отчитайки актуалните условия на киберсигурността, и да управлява екип с многостранни таланти. На практика обаче често ролята на CISO остава недоразбрана от бизнеса.

В крайна сметка как бизнесът може да се предпази, особено на фона на засилената дигитализация, на която станахме свидетели в последно време?

В едно изречение и с три И - информираност, инициатива и инвестиции, в защитата на най-критичните процеси, продукти (данни, устройства и системи) и хора.

Интервюто взе
Майя Бойчева-Манолчева

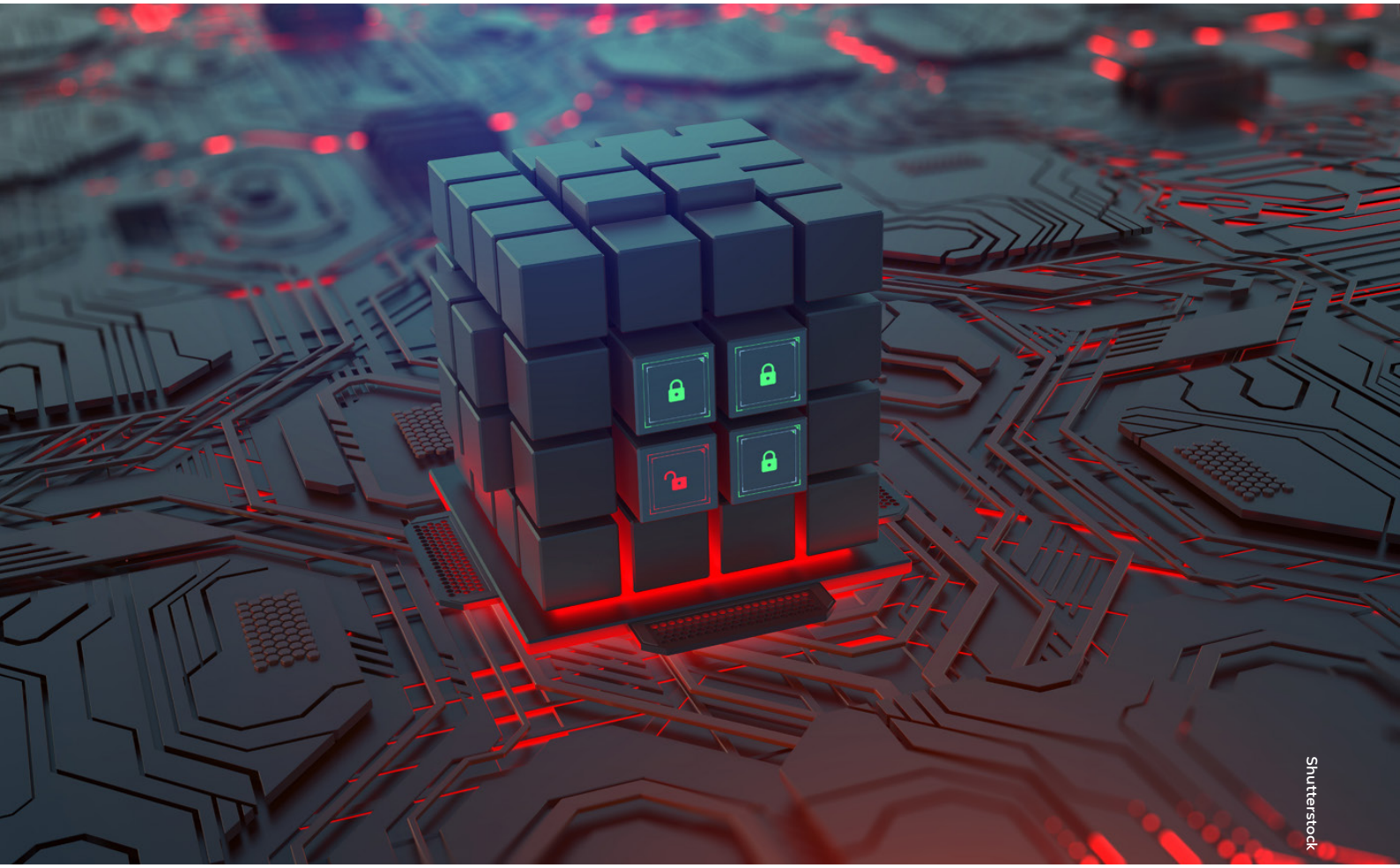
COLONNADE
A FAIRFAX COMPANY

Всеки може да се хване

Застраховката Кибер отговорност покрива фишинг и други онлайн опасности.

ПОЛУЧЕТЕ ОФЕРТА НА COLONNADE.BG

ПРОИЗВОДСТВЕНАТА ИНДУСТРИЯ ПОД КВАНТОВА ЗАПЛАХА



СПОРЕД ЧАСОВНИК НА CLOUD SECURITY ALLIANCE ЧОВЕЧЕСТВОТО ИМА СРОК ДО 14 АПРИЛ 2030 Г. ДА ЗАЩИТИ СВОЯТА ИТ ИНФРАСТРУКТУРА ОТ ДИГИТАЛЕН АПОКАЛИПСИС

Иван Гайдаров

През 2016 г. австрийският производител на аерокосмически компоненти FACC AG става обект на кибератака, която в крайна сметка му струва около 61 милиона долара. Атаката стартира като фишинг кампания от типа „китолов“, в която са таргетирани висши ръководители на компанията. В резултат на кампанията хакерите успешно се представят за изпълнителния директор на компанията и приключват сделка за придобиване на стойност 55.8 милиона долара.

Година по-късно Renault-Nissan е ударен с криптовируса WannaCry. Вследствие на претърпяната кибератака един от най-големите автомобилни производители спира работата на пет свои завода в Англия, Франция, Словения, Румъния и Индия. Компанията отказва да обяви официалните щети, но според анализаторите загубите, нанесени от този тип зловреден софтуер на производствената индустрия, достигат 4 милиарда долара.

През 2019 г. жертва на хакерите става Norsk Hydro. Производителят на алуминий с операции в 40 държави е принуден да затвори множество заводи след атака с криптовирус LockerGoga, която извежда от строя ИТ системите на различни бизнес функции, включително производствените процеси за топене в Норвегия, Катар и Бразилия. В крайна сметка атаката струва на Norsk Hydro приблизително 75 милиона долара.

И до днес това са едни от най-големите атаки срещу производствената индустрия и пример за това, че, от една страна, тя постоянно попада във фокуса на зловредните играчи, а от друга, че те са готови да използват широк инструментариум, за да постигнат целите си.

На този фон, с налагането на концепцията Индустрия 4.0 и очертаващите се контури на следващата версия - 5.0, все повече индустриални компании концентрират своите активи в дигиталното пространство, което изостря апетита на множество хакерски групи. Често ползващи се с подкрепата на различни държави, те имат достъп до сериозно финансиране и най-иновативните технологии. А това може да бъде изключително опасно за производствената индустрия в ерата на квантовите технологии, която чука на вратата.

КВАНТОВА ЗАПЛАХА

Наред с обещанията за научни революции и много нови възможности за бизнеса квантовите технологии отварят широко вратата и за нови заплахи. Експертите на американската неправителствена организация Cloud Security Alliance дори създават часовник за обратно броене - Years to Quantum (Y2Q) countdown clock, за да онагледят колко време има човечеството, за да защити своята ИТ инфраструктура в квантовия свят. Според него това трябва да се случи до 14 април 2030 г. В противен случай резултатът ще бъде само един - дигитален апокалипсис.

В своя съвместен доклад Transitioning to a Quantum-Secure Economy Световният икономически форум и Deloitte на свой ред посочват списък с конкретни заплахи за киберсигурността на предприятията, до които ще доведе развитието на квантовите възможности.

На първо място, анализът извежда заплахите пред комуникациите. „В днешния дигитален свят интернет трафикът и съобщенията в реално време са основна част от нашето работно ежедневие. Тези обмени се извършват в защи-

тени комуникационни канали, които използва алгоритми за криптиране с публичен ключ за обмен на уникален код за защита. Квантовите компютри могат да бъдат използвани за разбиване на този защитен канал и подслушване на практически всеки криптиран обмен. Това прави всички лични и тайни комуникации достъпни за злонамерените потребители“, категорични са анализаторите.

Целостта и автентичността на важни документи, които все по-често се съхраняват единствено в дигитален формат, също може да бъде компрометирана лесно чрез използването на квантови технологии.

„За определени видове данни (например поверителни и чувствителни), които имат както висока стойност, така и дълъг период на използване, квантовата заплаха може да се материализира под формата на атака, известна като „събиране сега, дешифриране по-късно“. При нея нападателите прихващат криптирани предавания на данни и ги съхраняват на твърд диск за по-късно използване. Дори едни криптирани данни да нямат значение към съответния момент, те могат да представляват интерес след 10 или 15 години, когато нападателят има достъп до криптографски подходящ квантов компютър. Това е от особено значение за регулираните индустрии, от които се изисква да съхраняват чувствителни данни на клиенти за дълги периоди от време“, акцентират авторите на Transitioning to a Quantum-Secure Economy.

Блокчейн технологията, която в момента набира все по-голяма популярност по отношение на киберсигурността като един от стълбовете на Индустрия 4.0, също се оказва, че не е достатъчно сигурен вариант за защита на чувствителна

информация. Блокчейн разчита в голяма степен на криптографски алгоритми за гарантиране на целостта на данните, транзакциите, обработката и доказване на автентичността. Според скорошни изследвания, цитирани в доклада на Световния икономически форум и Deloitte, обаче около 25% от наличните единици биткойн и 65% от етериум са уязвими на квантова атака, което означава само едно - блокчейн не е решение на новите предизвикателства.

КВАНТОВ ОТГОВОР

Такова все пак има и както често се случва, то идва от самия източник на заплахата. В случая - квантовите технологии.

Постквантовата криптография (PQC) използва нови криптографски алгоритми с публичен ключ, базирани на математически подход, които са проектирани да бъдат непробиваеми за атаки от алгоритъма на Шор (първия квантов алгоритъм за разлагане на цели числа на множители). PQC ще актуализира на фундаментално ниво настоящите алгоритми, които в един момент няма да бъдат достатъчно сигурни. Освен че се считат за достатъчно сигурни в квантовата ера, подобни възможности имат една допълнителна стойност - могат да бъдат внедрени в софтуерни решения в рамките на съществуващата инфраструктура.

Квантовото разпределение на ключове (QKD) разработва базирани на физиката квантови техники за генериране на сигурни комуникационни канали, които могат да се използват за разпространение на ключове за криптиране. QKD може да допълни използването на PQC и други криптографски алгоритми, като предостави защитен метод за разпространение на ключове.

Предимствата, които индустрията може да спечели от използването на QKD, включват както подобрена защита срещу атаки от типа „събиране сега, декриптиране по-късно“, така и възможност за изграждане на допълнителен слой сигурност в комбинация с други инструменти.

Квантовото генериране на произволни числа (QRNG) използва фундаментални квантови свойства за генериране на произволни числа - ключова част от криптографията.

Според Quantum Insider (TQI) общият пазар на квантова сигурност ще нарасне до близо 10 млрд. долара до 2030 г. при среден годишен ръст от 50%. Това показва, че индустриите оценяват заплахата, която носи квантовата ера, а от IBM напълно потвърждават тези опасения:

„Квантовите компютри се развиват бързо - може би дори по-бързо, отколкото можехме да предвидим преди пет години. Виждаме бързия темп на развитие на квантовата технология като голяма възможност. Вярваме, че тези машини ще решат важни проблеми в научните изследвания и индустрията. Че те ще ни помогнат да изградим по-добър свят. Но това бързо развитие води и до един важен извод - системите, които използваме днес за защита на чувствителни данни, няма да бъдат сигурни в свят, в който квантовите компютри са достигнали пълния си потенциал.“

СЪДЪРЖАНИЕ ОТ
kyndryl

Александър Николов,
Kyndryl

ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ ДОСТАВЯ ГЪВКАВОСТ И ИНОВАЦИИ, КАТО ИЗИСКВА ПОВИШАВАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

***Александър Николов** е изпълнителен директор на Kyndryl - България, доставчик на ИТ услуги, който стъпва върху наследството на IBM, за да подпомогне растежа и модернизацията на своите клиенти и партньори чрез внедряване на иновации и дигитални решения. Николов има над 20 години опит в ИТ сектора у нас, като през този период ръководи отдели „Развитие на бизнеса и продажби“, „Технически решения и доставки“, „Проектно портфолио и дигитални решения“. През 2017 е назначен за директор на IBM Global Technology Services в България, където допринася за разширяването на бизнеса в страната.*
Николов завършва Техническия университет в София с направление „Компютърни системи и технологии“, като продължава професионалната си квалификация с редица управленски и професионални обучения в London Business School, PWC и IBM training Academy.

Г-н Николов, на какво ниво е всъщност дигитализацията в банковия сектор в Югоизточна Европа и по-конкретно у нас?

Поръчано от Kyndryl изследване на компанията за пазарни проучвания SeeNews установи, че през 2021 г. топ 87-те банки в Югоизточна Европа похарчват приблизително 700 млн. евро за ИТ с нарастваща пропорция, инвестирана в нови дигитални услуги. Изследването също така показва, че макар банките в региона да инвестират засилено в ИТ, възвращаемостта от инвестициите им варира. Организациите с най-висока възвращаемост са тези, които имат цялостен подход към банкирането в дигиталната ера.

У нас дигитализацията в сектора е започнала с конкретни сегменти, разнородни в различните банки, но като цяло също липсва ясно изразена дигитална стратегия, която да върви с дългосрочен план за развитие и концепция по най-приоритетните теми. Финансовият сектор в България има критична необходимост от бърза цифровизация на всички бизнес процеси: от основните банкови такива, които са ритейл, корпоративни и онбординг на нови клиенти, до всички вътрешни, включително срещу пране на пари, картови разплащания и други бек офис процеси, тъй като много от тях все още са без системи или са неинтегрирани.

В този ред на мисли кои са основните двигатели, които мотивират банковите институции да се трансформират?

На първо място е потребителското поведение. Все повече хора използват телефоните си за плащания, търговия и всякакъв вид финансови транзакции. Новите привички и тенденции сред потребителите трансформират финансовите услуги. Според проучването на SeeNews всяка година повече от половин милион нови клиенти започват да разглеждат за нови дигитални предложения от тяхната банка, а търсенето на съществуващи и нови цифрови услуги нараства експоненциално.

На второ място са финтех компаниите, които предлагат гъвкави и лесно достъпни дигитални решения и дават възможности за дигитални финансови разплащания, какъвто е примерът с Revolut. До момента банковият сектор е изключително успешен, защото е бизнес на дове-

рие и гарантира, че доходите са на сигурно място. Вече с възможностите за дигитални комуникации, пазаруване и обмен на парични потоци, компаниите за индустриални облачни услуги (Hyperscalers) също започват да предоставят финансови инструменти. Това е основната причина, поради която банковият сектор бързо трябва да се дигитализира, за да може да настигне новаторите в този сегмент.

И на трето място, регулационните промени предизвикаха значителна дигитализация във финансовата индустрия, защото банките са задължени да съответстват и да отговорят на всички изисквания и правни норми на Европейската централна банка. Например ЕЦБ налага финансовите институции да имат възможност да са до голяма степен независими в техническите си решения. С други думи, търси се разнообразие от иновативни и бързи за внедряване и промяна решения. Такива биха предоставяли конкурентно предимство на проактивните в бранша, и това е тенденция, която ние виждаме в последните години. Води се така наречената гъвкава (agile) трансформация, която дава възможност на финансовите организации да участват в този процес, защото до този момент банките имаха бизнес звена, които се грижат за бизнеса, ИТ звена, които имлементират решения, и редица доставчици, които внедряват тези решения и ги поддържат във времето. В момента стремежът е трите страни да работят в синергия и с ясен фокус, а именно да се постигат по-бързо бизнес целите, да се изкарват банкови продукти на пазара в рамките на няколко седмици, а бизнес звената директно да комуникират с новаторите в бранша.

А какви рискове носи дигиталната трансформация за финансовия сектор и могат ли да се преодолеят?

Дигиталната трансформация е тясно свързана със сигурността. Тя води до повишен риск за информационната сигурност, а това налага да се имплементират специализирани решения. Системите за киберсигурност играят фундаментална роля в защитаването на днешното общество. Ориентирайки се към увеличаващата се дигитална работна среда, операционното, финансовото и репутационното влияние на кибератаките също се увеличава с глобален среден разход за пробив на данни, отчетен на 4.25 млн. долара.

Като мярка срещу затруднения с интеграцията на решения и услуги за сигурност индустрията направи крачка към стандартизиране и спецификация на тези сложни процеси. Така наречената „Отворена рамкова схема за киберсигурност“ (Open Cybersecurity Schema Framework) - общоприетият стандарт за споделяне на информация за киберсигурност, представен през август от индустриален консорциум на водещите технологични компании, звучи като решението, за което чакахме.

Проблемът тук е, че крачката към стандартизация ще пожъне успехи след известно време, а дигиталната трансформация продължава да предизвиква осезаема и неотложна нужда от инвестиции за сигурност и устойчивост.

В тази връзка не можем да не споменем и влиянието на Регламента за оперативна устойчивост на цифровите технологии. Какви са неговите изисквания и как финансовите институции могат да отговорят на тях?

Тази пролет Европейската комисия предприе първи стъпки към увеличаване на регулациите за подобрена ИТ сигурност в банки, застрахователни и инвестиционни компании. Регламентът за оперативната устойчивост на цифровите технологии (Digital Operational Resiliency Act) въвежда изисквания към участниците във финансовия сектор и техните ИТ доставчици за подсигуряване на издръжливост, реакция и възстановяване от всякакви видове ИТ атаки, включително способност да рестартират ИТ системите си в порядъчен период от време при случай на кибератака.

Няколко седмици след това Kyndryl бе една от първите компании в света, която предложи на пазара абонаментно решение, повишаващо способността за устойчивост на организациите във финансовия сектор. Recovery Retainer дава достъп до експертиза, дигитални активи и проактивна намеса от всички глобални ресурси на Kyndryl с цел незабавно стартиране на работата по възстановяването на системите и максимално съкращаване на времето от атаката до отново функциониращи операции.

За разлика от традиционните пакети срещу инциденти, които често предлагат криминалистичен анализ, Kyndryl се фокусира върху мерки за възстановяване като преинсталация на програми, определяне на процесите по въз-

обновяване на данни, системно почистване и други критично важни задачи. Подобни мерки адресират и другите нужди на клиента - да се намали негативният ефект от кибератаките, а услугата на Kyndryl се справя с атаки във всички видове среди - собствени физически, виртуални инфраструктури и в различни типове облачни решения.

Налични са три вида абонамента, като в двата премиум пакета са включени и проактивни обучения. Също така с превантивна цел Kyndryl може да извършва пробивни тестове, да тества риск осъзнаването на служители чрез социално инженерство или да проверява статуса на защитните стени на системите.

От технологична гледна точка кои тенденции ще определят развитието на банковия сектор през следващите години?

58% от ИТ лидерите в индустрията казват, че менажирането на инфраструктури изтощава ресурсите им, като лимитира техните способности да ускоряват иновациите си. Затова отговорът е опростяване на това как бизнесите избират, консумират и управляват дигитални технологии. Организациите по света все повече и повече търсят опростени продукти, за да имат възможността да „впрегнат“ силата на дигиталните инструменти и да „отключат“ нови бизнес възможности, оставайки конкурентоспособни.

Това важи в пълна степен за банковия сектор в региона и в България, където често организациите купуват един модул за основната им система и около него започват да

изграждат сателитни приложения, с които да са по-бързи, гъвкави и икономични, за да могат да обслужват цялото банково портфолио. Това създава палитра от десетки различни неинтегрирани и често архитектурно несъвместими решения за управление на една цяла банка. Този хаос трудно бива управляван дългосрочно във времето, следвайки нуждата за бързи промени и стабилно работещи системи. Банките биват притиснати от системните ограничения на технологично остарелите приложения.

Това поставя финансовите институции в ситуация, в която имат нужда от доверен партньор, който познава в детайли бизнеса, разполага с иновативни решения за покриването на неговите нужди и разполага с техническата компетенция да трансформира и мигрира съществуващите данни към новите апликации. Това върви ръка за ръка с оптимизацията на тези системи, така че да бъдат иновативни и лесни за употреба. Именно такава възможност предлага Kyndryl на своите клиенти. Kyndryl Bridge има за цел да осигурява бърз достъп до всички ИТ инструменти, от облачно изчисление, обработване на данни, анализ и изкуствен интелект, до решения за бизнес устойчивост заедно с основна инфраструктура и много други технологии.

В допълнение на опростяването платформата свързва потребители с експерти и технологични партньори на Kyndryl. По този начин финансовите институции могат да се фокусират по-малко върху управлението на ИТ системите и да освободят своите ИТ ресурси за работа с по-висока добавена стойност.

В заключение, каква е вашата прогноза за развитието на сектора през следващите години?

Технологичната модернизация ще бъде приоритет. 60% от ИТ директорите считат дигиталната трансформация за ключов фактор за растежа на организациите им, сочат данните на IDC. До 2023 г. всяка втора компания ще генерира повече от 40% от своите приходи от дигитални продукти и услуги, сравнено с всяка трета през 2020 г.

Затова можем да очакваме ръст на дигиталните нужди и тенденцията е за многократно ускорение на внедряването на дигитални решения за банките, а това върви ръка за ръка с повишаване на ИТ сигурността. Съхранявайки данните в дигитални масиви, даваме възможност за анализ и монетизирането на тези данни, от друга страна, повишаването на ИТ сигурността е от критична важност за оперативната цялост на всяка организация.

Shutterstock

ОБЛАЧНИТЕ ТЕХНОЛОГИИ СБЛИЖАВАТ СИГУРНОСТТА И МРЕЖИТЕ

КАКВО СЕ СЛУЧВА, КОГАТО ОБЛАЧНО БАЗИРАНИТЕ РАБОТНИ НАТОВАРВАНИЯ СЕ НУЖДАЯТ ОТ ЗАЩИТА, НО ТРАДИЦИОННИТЕ ПОДХОДИ НЕ ВЪРШАТ РАБОТА?

Владимир Владков

Центърът на тежестта за основните корпоративни данни се измести, като това важи и за голяма част от критичните за бизнеса приложения. Някога тези данни се съхраняваха само в корпоративен център за данни, докато сега има голяма вероятност те да се намират в облака. Скорошно

проучване от LogicMonitor установи, че 83% от работните натоварвания на предприятията вече са извън офиса.

Тъй като критична маса от приложения и натоварвания започнаха да се мигрират в облака, ИТ директорите се сблъскаха с факта, че мрежовите слоеве и слоевете за сигурност, свързващи крайните потребители с тези натоварвания, все още разчитат на остарели MPLS връзки. Скоро обаче цифровата трансформация се появи в дневния ред на всички бизнеси, тъй като хората търсеха мрежови решения, подходящи за съвременни цели.

Трансформацията към дигитални процеси беше сравнително бавен процес до началото на 2020 г., когато избухна пандемията от COVID-19. Тогава изведнъж се наложи всички да заработят от вкъщи и резултатът беше мащабна, но и хаотична промяна на ИТ екипите. Пътните карти за цифровизацията „се скъсиха“ за една нощ. Но всъщност COVID само наля допълнително „бензин в огъня“ за една тенденция, която вече беше налице - такава, която разделя печелившите от губещите в утрешната дигитално управлявана икономика.

На този фон ИТ директорът се е превърнал в много случаи в най-важния човек в една организация. В един дигитално трансформиран свят ИТ директорът е този, който държи ключовете за толкова много решения: вътрешни и външни комуникации, сътрудничество и способността да се даде възможност за всичко - от дистанционна работа до извършване на сливания и придобивания по възможно най-бърз и безболезнен начин.

Към сложната комбинация от съвременни технологични

проблеми се добави „безмилостният“ ритъм на опасенията за киберсигурността. Наследените мрежи правят хората уязвими към ужасяващи заплахи като атаки с криптовируси (ransomware). Съществува и неприятният факт за осакатяващия недостиг на таланти за мрежова сигурност, което добавя още по-голяма турбуленция към перфектната буря от предизвикателства. Явно трябва да се намерят нови начини за трансформиране на свързаността далеч от наследеното минало, като в същото време сигурността се интегрира по-ефективно в мрежата, без да се хвърлят огромни суми за проблема или да се опитвате да се наемате експерти (които не съществуват), които да свършат работата.

НОВИ НАСОКИ ЗА SASE

В този контекст е важно да се отбележи еволюционното развитие на пазара за решения за защитен достъп до периферни услуги (SASE), технология, често цитирана като панацея за предизвикателствата, свързани със сигурността и работата в мрежа. Терминът е предложен от Gartner през 2019 г., но след това SASE бързо се изкачи до върха на дневния ред на ИТ, макар и „леко помрачен“ от превръщането му в оборкващ пазар, където очевидно подобни, но всъщност подчертано различни продукти се борят за вниманието на ИТ директорите и директорите по киберсигурност (CISO).

Като се има предвид, че няма един вариант на SASE, който да пасва на всички, трябва да се вземат „информирани“ решения. Важно е да се осъзнае например, че когато става дума за архитектура на SASE, доставчиците на технологии са склонни да възприемат подход, базиран на рамка или

на продукт. Някои възприемат и двата подхода.

При рамковия подход, който ние наричаме „дезагрегиран SASE“, отделни мрежови технологии и технологии за сигурност са интегрирани в цялостното внедряване на SASE

Маурисио Санчес, директор „Мрежова сигурност“, SASE в Dell'Oro Group

„При рамковия подход, който ние наричаме „дезагрегиран SASE“, отделни мрежови технологии и технологии за сигурност са интегрирани в цялостното внедряване на SASE - отбелязва Маурисио Санчес, директор „Мрежова сигурност“, SASE, SD-WAN в независимата анализаторска фирма Dell'Oro Group. - Мрежовите технологии и технологиите за сигурност може да идват от един и същ доставчик или от различни доставчици на SASE. Обикновено дезагрегираните реализации се състоят от множество хранилища на политики - по едно за всяка мрежа или за всяка услуга за сигурност. Това разграничение е важно при сравнение с продуктовия подход“, добавя Санчес.

Втория подход Маурисио Санчес дефинира като Unified SASE. При него „всички мрежови технологии и технологии

за сигурност са внедрени като единна, тясно интегрирана продуктова платформа само с едно хранилище на политики, обхващащо политиката и за мрежата, и за сигурността“.

В сравнение с дезагрегирания подход Unified SASE има множество предимства, обхващащи и технологичния, и икономическия спектър, коментира Санчес. „Например множеството хранилища на политики в дезагрегирания SASE може да изискват ръчно и понякога трудно съгласуване на политики от администраторите, което унифицираната SASE избягва заради по-монолитното му внедряване“, обяснява той. Той отбелязва, че предприятията, на които им липсват специализирани ИТ екипи за мрежите и за сигурността, често избират унифицирани внедрявания поради по-голямата простота на този тип решения.

Една от компаниите, прилагащи унифицирания подход към SASE, е Aryaka. Неговата WAN услуга Zero Trust, базирана на унифицирани принципи на SASE, сега включва защитен уеб портал и защитна стена като услуга. Компанията твърди, че интеграцията е първата по рода си, която позволява на предприятията да налагат политики за сигурност и в офиса, и за отдалечени потребители с унифициран контрол, като същевременно осигурява производителност и стабилна работа на приложенията.

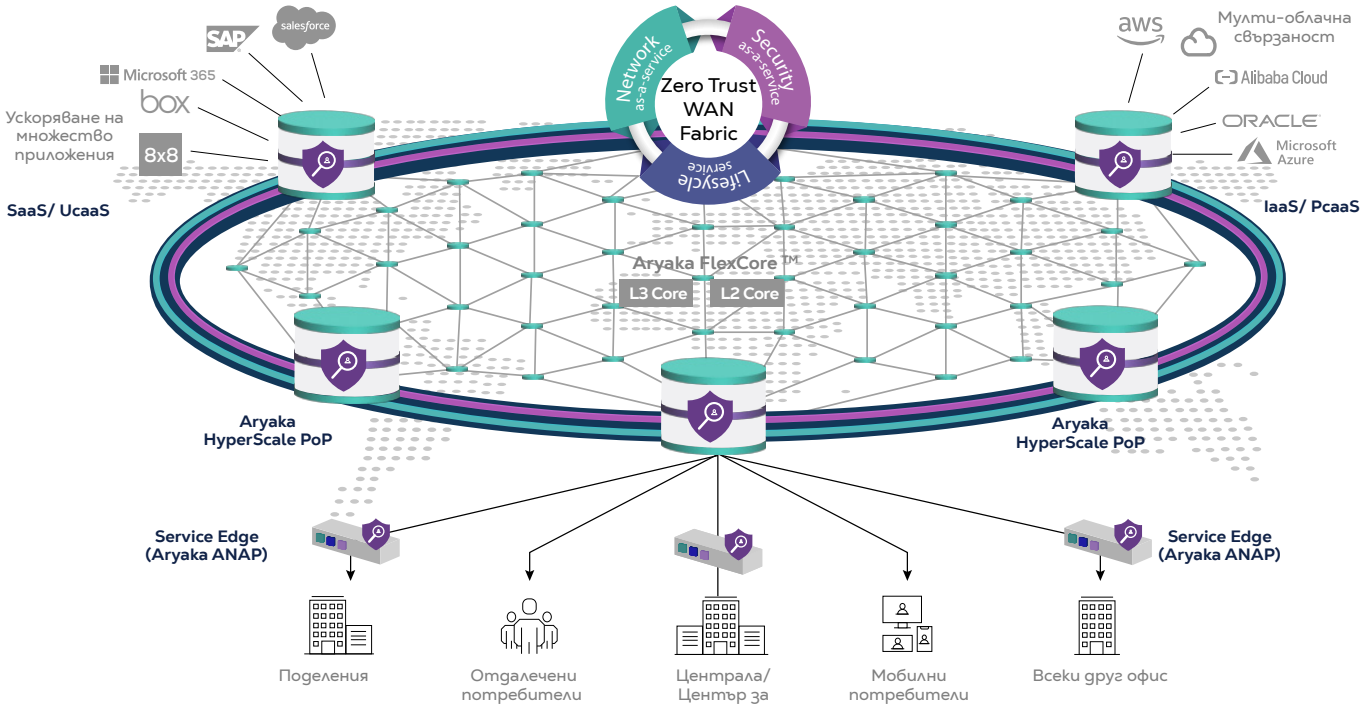
Дейвид Гинсбърг, маркетинг вицепрезидент в Aryaka, твърди, че е важно да се подходи към сигурността с принципите на „нулево доверие“, но без да се жертва производителността на приложенията. „За да балансирате наистина и двете, се изисква интегриране на сигурността и мрежата в обща платформа за наблюдение, управление, налагане на правила и оптимизиране - казва той. - Сега

можете сигурно да свържете всеки потребител навсякъде по света през глобален, софтуерно дефиниран „гръбнак“ с интегрирана сигурност в периферията за достъп до работни натоварвания, където и да „живеят“ те“, допълва Гинсбърг.

Глобална мрежа WAN с нулево доверие включва прилагане на принципите на нулево доверие от гледна точка на сигурността, но след това и на свързването на потребителя в мрежата. „Не можете просто да поставите отгоре слой за сигурност - казва той. - Това трябва да стане част от начина, по който управлявате мрежата. Нуждаете се от истински баланс между сигурност и работа в мрежа, така че повишената сигурност да не влошава продуктивността. Видимостта също е ключова, тъй като всичко се управлява от единен контролен панел.“

УНИФИЦИРАН SASE

Решение тип „всичко в едно“ съчетава SD-WAN и сигурност и ги предоставя като услуга



Визията на Aryaka съвпада с дефиницията на Dell'Oro, която я признава за най-новия технологичен доставчик, който доставя унифицирано SASE решение, комбиниращо сигурност и мрежова свързаност. Другите три доставчика в това пространство са Cato Networks, Versa Networks и VMWare.

Aryaka е и единственият доставчик на управлявани услуги, който получи обозначението Customer Choice от анализаторската фирма Gartner в последния си доклад Peer Insights за Северна Америка, EMEA и Азиатско-Тихоокеанския регион. Според Gartner периферната WAN инфраструктура сега трябва да включва разширяващ се набор от мрежови функции, включително защитени рутери, защитни стени (Firewall), SD-WAN, контрол на WAN връзките и WAN оптимизация заедно с традиционната функционалност за маршрутизиране.

ЦЯЛОСТЕН ПОДХОД

Друг поддръжник на унифициран подход към мрежите и сигурността е Кристофър Родригес, директор изследвания в IDC: „Модернизацията на сигурността е фундаментално изискване предвид множеството нови технологии в корпоративните ИТ среди днес, както и заради многобройните участници в заплахите, които са готови да се възползват от всяка грешка - отбелязва той. - Фокусирането върху стратегия за трансформация само на мрежата води до изолиран подход към сигурността, който се оказа неефективен при предишни итерации. Цялостният подход към трансформацията на мрежата и сигурността осигурява ключови ползи за бизнеса, но и технологични предимства, които позволяват истинска цифрова трансформация.“

Той вярва, че е необходим съгласуван план за конвергенция на мрежата и сигурността за внедряване на SASE, което е изгодно както от гледна точка на сигурността, така и на мрежата: „Пътната карта ще изглежда различно за всяка компания, но като цяло организациите могат да се възползват от решение, което позволява прогресиращо внедряване“, заключава той.

ПЕРСПЕКТИВИ

В бъдеще може да се получи сближаване на мрежите и сигурността, базирани около единна равнина на управление, равнина на разпределени данни и хостван в облак контрол. Това ще позволи на предприятието да оптимизира предоставянето на сигурно и стабилно работещо приложение. Що се отнася до SASE, вероятно конвергенцията на мрежите и сигурността ще бъде отправна точка към ново поколение продукти, които разширяват периферията на облака до тази на предприятието, заедно с необходимостта за предоставяне на последователно изживяване и безпроблемен контрол през облака и през инсталациите на място, в предприятието.

akat

akat-t.com

Shift your IT security and operations to a new level

Cut the cost Embrace the future

Security breaches do not occur because there are no firewalls and security solutions in place. They do rather occur because of mis-configurations and omissions.

We are the experts to provide you with understanding and guarantee your control.

ЕДНА ЧЕТВЪРТ ОТ КОМПАНИИТЕ СА ЖЕРТВА НА РАНСЪМУЕР АТАКИ

Shutterstock

МИГРАЦИЯТА В ОБЛАКА И ФАЛШИВОТО УСЕЩАНЕ ЗА СИГУРНОСТ НА ЕКСПЕРТИТЕ СА СРЕД ПРИЧИНИТЕ ЗА УСПЕХА НА ХАКЕРИТЕ

Мария Динкова

24% от компаниите са станали жертва на рансъмуер атака, като една пета са се случили през последните 12 месеца, показва новото проучване на Hornetsecurity: The 2022 Ransomware Report. Според данните от изследването, проведено сред над 2 хил. ИТ мениджъри на компании от различни индустрии и континенти, продължаващата миграция в облака и фалшивото усещане за сигурност на експертите, са сред основните причини за успеха на хакерите.

„Атаките срещу бизнеса се увеличават и има шокираща липса на разбиране и подготвеност от ИТ специалистите“, коментира Дениъл Хофмън, главен изпълнителен директор на Hornetsecurity. По думите му голяма част от ИТ общността има фалшиво чувство за сигурност, а злонамерените актьори разработват нови техники, с които да заплашват компаниите.

Тазгодишните данни потвърждават, че темповете на рансъмуер атаките не само се запазват, но и се повишават. Този тип нападения се превръщат във все по-честа заплаха за компаниите, а тази година се наблюдава увеличение от 3% спрямо 2021 г., когато от такива инциденти са пострадали 21% от фирмите.

Според авторите на доклада този ръст се дължи на две основни причини. На първо място е фактът, че тези нападения продължават да бъдат печеливши за киберпрестъпниците, а организациите се затрудняват да се защитят. На второ място експертите посочват повишеното използване на хибридни облачни технологии. Повечето ИТ екипи разчитат на платформи като Microsoft 365 и Google Worspace, смятайки, че вградените опции за сигурност ще ги защитят изцяло от заплахи.

ОБЛАЧЕН РИСК

Един от основните изводи от доклада е, че на бизнеса му липсват знания за инструментите за сигурност. Една четвърт от ИТ експертите или не знаят, или не мислят, че данните в Microsoft 365 могат да бъдат засегнати от рансъмуер атака. В реалността обаче незащитените облачни платформи са също толкова уязвими, ако не и повече в сравнение с ИТ инфраструктурата в инсталациите.

В същото време 40% от ИТ специалистите, които използват Microsoft 365 в своята организация признават, че нямат план за възстановяване, в случай че техните данни бъдат компрометирани от рансъмуер атака. През 2021 г. 16% от запитаните са посочили, че нямат подобна стратегия, докато тази година тези стойности достигат 19%, въпреки увеличената честота и брой на атаките.

А решението е доста логично, освен надежден план за възстановяване, компаниите се нуждаят и от инструменти на трети страни, с които да защитят своите системи. Това е задължително, като се има предвид, че над половината от ИТ експертите предвиждат до 5 години тяхната фирмена ИТ инфраструктура да бъде изцяло или предимно в облака.

НЕПЛАНИРАНЕТО ИЗЛИЗА СКЪПО

Съвсем логично липсата на подготвеност от страна на ИТ експертите и бизнеса в крайна сметка излиза доста скъпо. Често обаче загубите не са само финансови, но също така засягат имиджа на бранда, вредят на потребителското изживяване и затрудняват работните процеси.

Проучването разкрива, че над една пета от компаниите, които са били нападнати, са платили или изгубили данните си. Именно защото има значителен шанс да им се плати, хакерите извършват подобен тип атаки. Всъщност 7% от ИТ специалистите, чиито организации са пострадали, признават, че са платили откупа, докато 1 от 7 (14%) отбелязват, че са загубили данните си в резултат от атаката.

СКЪПОСТРУВАЩИТЕ ПРОБИВИ

В тези стойности се взимат под внимание не само платените откупи, но също така разходите заради спирането на дейността и индустриалните глоби, ако компаниите не успяват да защитят чувствителни данни.

изследване на IBM

Интересно е да се отбележи, че в същото време 97% от експертите са сравнително или изключително уверени в своя основен метод за защита, дори да не използват много от най-ефективните мерки за сигурност. Според ав-

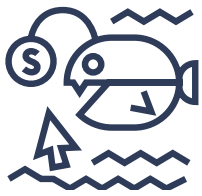
торите на доклада тази тенденция ясно показва нуждата от повече обучения в сектора.

НАЙ-ЧЕСТИТЕ АТАКИ

Почти 6 от 10 докладвани рансъмуер нападения (58.6%) са резултат от зловреден имейл или фишинг атака. Тези цифри не са изненадващи, след като според изследването 27% от организациите не осигуряват обучения на крайните потребители как да разпознават и откриват потенциални рансъмуер атаки. Освен това само 61.4% от компаниите използват технологии за филтриране на имейли и анализ на заплахите.

„Киберпрестъпните винаги ще се насочат към най-слабото звено от ИТ инфраструктурата и в повечето случи това е крайният потребител. Миналата година, проведохме изследване, фокусирано върху имейл сигурността, което установи, че 62% от пробивите в имейл сигурността са причинени от компрометирани потребителски пароли и успешни фишинг атаки“, отбелязват авторите на доклада. По думите им това ясно показва, че за да се предотвратят рансъмуер атаките, ИТ експертите трябва да се фокусират преди всичко върху потребителите.

ИЗТОЧНИЦИ НА РАНСЪМУЕР АТАКИ



58.6%
зловреден имейл или фишинг атака

16.4%
компрометирани крайни точки

7.7%
лоша сигурност на периметъра

7.2%
социално инженерство

6.4%
атаки от типа нулев ден

6.4%
други

А повечето от тези кибернападения имат една цел – сървърната инфраструктура и мрежовия сторидж. Именно това са засегнали рансъмуер атаките при 56% от анкетираните, вероятно с цел криптиране на критични данни. Сред другите цели на хакерите ИТ експертите посочват множество крайни точки (36%) и единична крайна точка (35%). Отделно 1 от 7 запитани (15%) отбелязват, че хакерите са насочили своите усилия срещу фирмените бекъпи.

ПРЕДОТВРАТЯВАНЕ НА РАНСЪМУЕР АТАКИ

Макар организациите да разполагат с решения за защита, когато става въпрос за рансъмуер е особено ключово какви действия предприемат, за да предотвратяват на първо място подобни атаки. Изследването разкрива, че най-често организациите прибягват до технологии като софтуер за откриване в крайната точка с антирансъмуер възможности (69%), а също така филтриране на имейли и анализ на заплахи (61%).

В този ред на мисли интересна е тенденцията за спад в популярността на този тип решения в сравнение с данните от предходната година. През 2021 г. 76.6% от организациите са използвали софтуер за откриване в крайната точка, и 76.2% са разчитали на инструменти за имейл фил-

триране. Според авторите на доклада това понижение се дължи на преминаването към облачни платформи и вследствие на това много компании започват да разчитат на вградените защити, отколкото да предприемат проактивен подход за предотвратяване на рансъмуер атаки. Не на последно място, трябва да се отбележи, че

Част от компаниите разчитат и на специфични застраховки, покриващи риска от кибератаки.

са купили подобни продукти

Според специалистите от Hornetsecurity трябва да се подхожда внимателно в този случай, тъй като някои застраховки могат да изискват определени превантивни мерки, за да бъдат получени, а това може да се окаже скъпо начинание като цяло.

ВАРИАНТИТЕ НА РАНСЪМУЕР СЕ УВЕЛИЧАВАТ

Не само компаниите обаче инвестират в справяне с киберзаплахите, но също средства за подобряване на своите възможности отделят и хакерите. През първата половина на тази година са засечени 10,666 рансъмуер разновидности в сравнение със само 5,400 през предходните шест месеца, показват данните на FortiGuard Labs. Това означава почти 100% ръст в рамките на две тримесечия и е знак за бързо еволюиращите престъпни екосистеми.

Една от причините за тази тенденция е нарастващата популярност на рансъмуер като услуга (RaaS) в тъмната мрежа. Чрез подобни решения дори и сравнително неопитни престъпници могат да извършват печеливши рансъмуер атаки.

Данните от тазгодишното изследване са еднозначни – рансъмуер атаките продължават да представляват сериозна заплаха за бизнеса, независимо от големината на компаниите или сектора, в който работят. Увеличените темпове на атаките и фактът, че 1 от 20 ИТ експерти се е сблъскал с този тип кибернападение през последните 12 месеца, определено ги превръща в предизвикателство. В този смисъл фирмите трябва да останат бдителни особено при миграция към облачни платформи.

„Макар облачните технологии да осигуряват значителни ползи по отношение на удобство и изисквания за поддръжка, те налагат нуждата от силно проактивен подход към сигурността, за да се минимизира заплахата от кибератаки и да се предотвратят рансъмуер инциденти“, съветват авторите на доклада. Това на свой ред включва предприемането на мерки за видимост и защита в реално време, комбинирани с мрежови достъп с нулево доверие и модерни решения за откриване и реакция на крайната точка.

ЗАЩО В ДНЕШНИЯ СВЯТ ВСЯКА КОМПАНИЯ СЕ НУЖДАЕ ОТ ЗАСТРАХОВКА „КИБЕРОТГОВОРНОСТ“?

Киберпрестъпленията и течовете на данни за много компании вече не са абстрактен проблем, с който никога не биха се сблъскали в реалността или от типа „това на нас няма да ни се случи“. В началото на октомври, по време на старта на Европейския месец на киберсигурността, бяха изнесени данни, че 57% от организациите у нас са подложени на ежеседмични фишинг атаки. А

това обикновено е първата стъпка на рансъмуер кампаниите, които представляват най-значителната заплаха за бизнесите през последните години. Ръстът в сферата е експоненциален за последното десетилетие и се очаква да достигне 10 млрд. долара до 2025 г. По данни на Агенцията на Европейския съюз за киберсигурност (ENISA) в над 60% от случаите на атаки с криптовируси следва изтичане на данни.

НЕ ПРОСТО ЗАГУБА НА ИНФОРМАЦИЯ

На този фон киберзастраховането придобива все по-съществено значение за всички компании, тъй като рискът от кибератаки срещу фирмените приложения, устройства, мрежи и потребители нараства ежедневно. Паралелно с това компютърните системи и цифровият имидж на организациите стават все по-критични за тяхната работа. Често кражбата на данни може не просто да повлияе временно на бизнеса, но да причини и значителна загуба на клиенти, репутация и приходи.

Предприятията носят наказателна отговорност за щети, причинени вследствие на теч на данни от трети страни. Затова политиките за киберзастраховане защитават от непредвидени киберсъбития. Също така, въпреки че на киберсигурността обикновено се гледа като на технологичен проблем, повечето от пробивите с изтичане или кражба на данни са резултат от човешка грешка - риск, който е много труден за контролиране и предвиждане. Затова застраховката може да е единственото средство за ограничаване на щетите.

РЕШЕНИЕТО

За да отговори на развиващата се динамична дигитална среда и за да помогне на клиентите си да бъдат по-уверени в морето от технологични възможности и свързаните с тях постоянно появяващи се нови заплахи, „Колонад Иншуърънс“ предлага застраховка „Киберотговорност“ като актуално полезно решение за бизнеса.

Тя осигурява покритие при кибератаки и физическа кражба на данни, както и покрива претенции за загуба на информация. Възстановяват се и направените разходи при изтичане на данни, свързани с административни процедури до съответния подлимит.

Основните преимущества, които е добре да търсите в такъв продукт, за да е максимално ефективен за вашия бизнес, са:

- *Да осигурява покритие както за застрахования, така и за засегнатите трети лица. Да покрива разходите за съдебна защита.*
- *Да покрива всяка претенция за загуба на информация, която съгласно местното законодателство се счита за „лична“ или загуба на „корпоративна информация“.*
- *Да възстановява разходи, свързани с административни процедури до съответния подлимит, посочен в полицата.*
- *Да покрива разходите за експертни специалисти по киберрискове, разходите за консултации и препоръки относно връзките с обществеността, разходите за възстановяване на репутацията на физическо лице.*

В основното покритие на застраховката на „Колонад“ влиза още отговорност при аутсорсинг (обработка от трети страни) - при претенция за загуба на информация от подизпълнител, който съхранява или събира лични данни за застрахования.

Допълнителни премии пък могат да покриват рискове от киберизнудване и прекъсване на компютърни мрежи. Киберизнудване за лични данни например включва щети, свързани с атакуване на компютърна система с цел искане на пари. Пример за това е, ако хакери атакуват информация, която застрахованият смята за ценна и фактически бива изнудван заради нея. Друг пример са заплахи за пускане на

кампании от типа „отказ от обслужване“ (DDoS).

Киберзастраховките започнаха да стават по-масова тема едва през последните години, като причина за това са все по-честите съобщения за атаки и изтичания на критични данни, както и отминаващата ковид криза и свързаното с нея масово преминаване към режим на дистанционна работа за огромен брой служители. Не на последно място обаче и традиционните застрахователни продукти, насочени към бизнеса, не са в състояние да покрият новопоявяващите се рискове, свързани с киберсигурността и нейните специфики.

Затова изборът на правилен доставчик за такъв продукт е от особено значение. „Колонад Иншуърънс“ („Колонад“) е застрахователна компания, базирана в Люксембург, развиваща дейност в сферата на общото застраховане, установена чрез клон в България. Собственост е на холдинга Fairfax и е учредена с цел стратегическо разширение на застрахователния му бизнес в страните от Централна и Източна Европа. „Колонад“ е една от малкото компании в региона с инвестиционен кредитен рейтинг (A- от AM Best). От компанията са си поставили за цел да предлагат най-адекватното застрахователно решение в точния момент и според конкретните и специфични нужди на клиентите и партньорите си и продуктът „Киберотговорност“ е доказателство за това.

„Колонад Иншурънс Ес Ей “

1407 София, Промишлена зона Хладилника,
Феърплей бизнес център, бул. „Черни връх“ 51Б

info@colonnade.bg

тел.: +359 2 930 9330

www.colonnade.bg

5 СЕКТОРА, КОИТО НАЙ-ЧЕСТО СТАВАТ МИШЕНА НА КИБЕРАТАКИ

ПРОИЗВОДСТВО, ФИНАНСОВИ ИНСТИТУЦИИ, ЗДРАВЕОПАЗВАНЕ, ОНЛАЙН ТЪРГОВЦИ И ПРАВИТЕЛСТВЕНИ ОРГАНИЗАЦИИ СА СРЕД НАЙ-ЗАСТРАШЕНИТЕ

Майя Бойчева-Манолчева

Shutterstock

Киберпрестъпленията в глобален мащаб следват твърдо тенденциите на развитие на секторите и степента на навлизане на технологиите в тях. Колкото по-технологично иновативен е един сектор, толкова по-често мишена на атаките е той. И това е лесно обяснимо, като се има предвид старата максима, че най-добре защитеното устройство е това, което е изключено от мрежата. В последните две години два ключови фактора оказаха влияние на киберсигурността - пандемията и последвалата дигитализация и войната в Украйна. Кои са петте сектора, които са най-застрашени от кибератаки?

ПРОИЗВОДСТВО

Според доклада на IBM „Security X-Force Threat Intelligence Index 2022“ през 2021 година производственият сектор е претърпял повече атаки от финансовия. В Европа например 25% от атаките са насочени към него, 18% - към финансовия и застрахователния сектор, и 15% - към бизнес услугите. 23% от тези атака са били чрез рансъмуер. 61% от инцидентите, свързани с оперативните техно-

логии (ОТ), са били в производството, а 35% от атаките към организациите, свързани с ОТ, са били рансъмуер. Причината производственият сектор да е толкова примамлив за този тип заплахи е фактът, че индустриалните предприятия не могат да си позволят дълго време да са извън строя и лесно биха се поддали на искането за плащане на откуп.

Производственият сектор обикновено не влиза в докладите за киберсигурност, но с разпространението на заплахите към веригите за доставки това се промени. Затова и другата тенденция, която се забелязва, е, че уязвимостите са били основен вектор за атака в сектора през миналата година, като така са поставяли под риск цялата верига за доставки. Повечето производители вече използват автоматизация, IoT и други свързани технологии, което изисква гарантиране на високо ниво на сигурност на тези устройства.

ФИНАНСОВ СЕКТОР

74% от финансовите институции е трябвало да се справят с кибератаки, свързани с пандемията, сочат данните на AT&T Business. Според IBM и института Ponemon средната цена на изтичането на данни във финансовия сектор през 2021 година е била 5.72 млн. долара.

Като основна заплаха тук стои добре познатият ни стар фишинг, при който се подмамват потребителите да дадат своите данни, а най-разпространеният вид е „имейл фишингът“. Ценността на събираните данни пък прави сектора изключително притегателен за рансъмуер заплахи. На трето място като използвани методи за

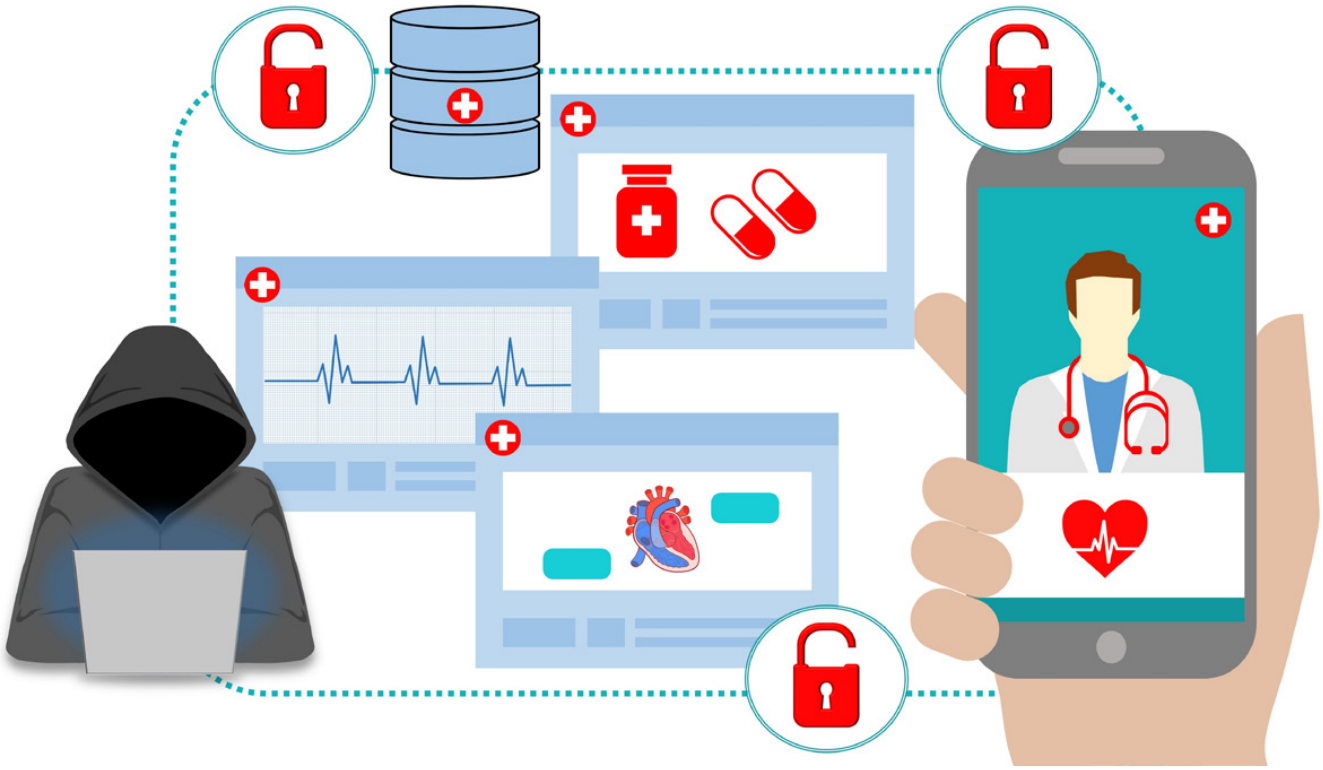
Shutterstock

атака се нареждат SQL инжекциите (SQLi), кръстосаното скриптиране на сайтове (XSS), атаката тип „локално включване на файлове“ (LFI) и OGNL Java инжекциите. Четвъртият метод, който използват киберпрестъпниците, е DDoS. През 2020 година DDoS атаките срещу финансовия сектор са нараснали с 30%. Освен репутационните проблеми и недоволните клиенти DDoS атаките ангажират вниманието на голяма част от екипа по киберсигурност, което отваря вратите на киберпрестъпниците за реализирането на друг тип престъпления.

Анализаторите са категорични, че атаките към финансовия сектор ще продължават да нарастват главно поради голямата дигитализация и широкото навлизане на онлайн банкирането.

ЗДРАВЕОПАЗВАНЕ

Този сектор е често мишена на кибератаки, като основната причина за това е, че използва огромно количество данни, включително лични данни и финансова информация. Добър пример е атаката с рансъмуера WannaCry срещу британската национална здравна служба (NHS) през 2017 година. В резултат от нея бяха отменени 19 000 прегледа за период от една седмица, което е струвало на здравната организация 92 милиона паунда. 80 болници и 8% от дейността на личните лекари са били засегнати.



Shutterstock

COVID-19 още повече стимулира киберзаплахите към здравния сектор. Хакерите бързо осъзнаха, че пандемията привлича огромни парични потоци към индустрията. Доставчици, институции и бизнес организации се превърнаха в мишена на киберпрестъпления. Данните на па-

циентите са високо ценени и лесно продавани в Тъмната мрежа и мрежите на киберпрестъпниците, тъй като позволяват кражба на идентичност.

Телемедицината допълнително увеличава опасността от грешки и пролуки в сигурността и експертите са категорични, че сигурността тук трябва да се гарантира на всяко ниво - парола, устройство, файл и потребител.

ОНЛАЙН ТЪРГОВИЯ

Пандемията от COVID-19 и ограниченията, които бяха наложени, сътвориха небивал бум в онлайн търговията, което, разбира се, поведе след себе си и доста проблеми със сигурността. С нарастването на е-търговията през 2020 година киберпрестъпленията също скочиха и

Shutterstock

в резултат анализаторите отчетоха загуби в размер на 1 трилиона долара. Според данните секторът понася 32,4% от всички успешни заплахи годишно. Цел на хакерите обикновено са администраторите на магазините, потребителите и служителите. Най-разпространените заплахи в сектора остават финансовите измами, включително измамите с кредитни карти и фалшиви искания за връщане на стоки и възстановяване на пари. Популярният фишинг и в този сектор е на мода, като потребители алармират за получени имейли, водещи към фалшиви копия на сайта и опитващи се да измъкнат финансова информация от клиентите.

Изпращането на спам имейли със заразени линкове също е характерен метод на атака, който се използва в сектора, както и популярните DDoS атаки, за които вече стана дума.

ПРАВИТЕЛСТВЕНИ ОРГАНИЗАЦИИ

Атаките към държавните институции и международните организации също бележат ръст, като особено отчетливо се вижда това на фона на войната в Украйна.

Всички помнят срещата на Г-20 в Париж през 2011 година, когато имейл с прикачен заразен pdf, изпратен до министерството на финансите на Франция, доведе до 150 заразени компютъра и достъп до конфиденциална информация на Г-20. През 2015 година 16 германски депутати, включително канцлерът Ангела Меркел, станаха обект на атака и разкриване на информация. Разбира се, и България не остава по-назад. Емблематична беше хакерската атака срещу НАП през 2019 година, при която изте-

коха данните на около 5 млн. български и чуждестранни граждани.

Много често атаките срещу държавните институции целят достъп до конфиденциална информация или са политически обусловени. В последните месеци правителствени сайтове на различни държави станаха обект на DDoS атаки, зад които стоят държавно спонсорирани хакерски групи.

Стефан Джурелов,
„Тинк Смарт“

АКО НЕ ИНВЕСТИРАМЕ В КИБЕРСИГУРНОСТ, СМЕ ОСТАВЕНИ НА ТЕЧЕНИЕТО

***Стефан Джурелов** заема позицията на управител в „Тинк Смарт“. Той има над 25-годишен опит в ИТ бизнеса. През 2020 г. създава „Тинк Смарт“ и оттогава активно развива компанията. Днес в нея работят над 20 служители, като екипът продължава да се разширява, наемайки и обучавайки млади и ентусиазирани експерти.*

Г-н Джурелов, какви са водещите тенденции в сферата на сигурността, които в „Тинк Смарт“ наблюдавате през тази година?

През последните 2 години сме свидетели как дигитализацията в редица сфери от нашия живот бе ускорена от Ковид-19 пандемията. Честно казано това, което не можахме да направим за 10 години, го прескочихме само за 2. Това е едно от положителните последствия от пандемията. Високотехнологичните иновации са от ключово значение днес. Определено всички си даваме сметка, че ако не инвестираме в киберсигурност, сме оставени на течението и рано или късно то ни повлича.

Какви са основните трудности, с които компаниите днес се сблъскват при управлението на своята сигурност и гарантирането защитата на данните си?

Ясно е, че да сме в крак със заплахите, трябва да обновяваме, както хардуерните си ресурси, така и софтуерните такива. За нас в „Тинк Смарт“, човешкият фактор е от особено значение. Опитваме се да развиваме не само нашите специалисти, но също така и компетенциите на самите клиенти, защото зад всяка услуга стои жив човек и е важ-

но и двете страни да знаят какво правят и как го ползват. Инвестираме в обучение на нашите колеги и в повторяеми обучения при клиенти. Информацията е най-ценният ресурс през XXI век и нашата обща задача е да я пазим с всички позволени хардуерни и софтуерни средства.

В този ред на мисли за какви киберрискове трябва да са подготвени организациите? Какви са основните грешки, които фирмите често допускат?

Като че ли свикнахме последните месеци, че можем да бъдем обект на атаки. Клиентите вече осъзнават какво може да загубят и инвестират в технологии. Не знам дали е грешка, но определено е възможност за развитие да се обръща внимание на докладите, анализите и препоръките, които са резултат от работата на екипите по киберсигурност и от възможностите на съвременните технологии. И най важното е да правим своевременни промени в начина на работа на базата на споменатите вече препоръки.

Как „Тинк Смарт“ подпомага бизнеса при осигуряването защита на фирмените ИТ инфраструктури?

От няколко години се говори за SaaS - сигурност като услуга (security as a service), и повечето от българските ИТ компании инвестират в тази посока - както в необходимите технически ресурси, така и в човешкия потенциал. Сигурно ще прозвучи тривиално, но екипите ни са квалифицирани и с необходимия потенциал, за да предоставим качествени услуги на нашите клиенти. Разчитаме на сплав от опита на по-възрастните колеги и въображението на по-младите, което е предпоставка за успех. Наскоро

стартирахме кампания „Работилница за киберталанти“ за ученици от 14 до 19 години. Нашата надежда е младото поколение и затова искаме заедно още от училище да се развиваме, за да можем след години и да работим заедно.

Какви решения най-често търсят организациите при вас?

Защитна стена като услуга е много търсено решение през последното шестмесечие, но също така имаме увеличение на запитванията и внедряванията при клиенти на системи за управление на уязвимости.

В заключение, какъв съвет бихте дали към компаниите, които искат да подобрят своята ИТ сигурност? Кои са първите стъпки в тази посока?

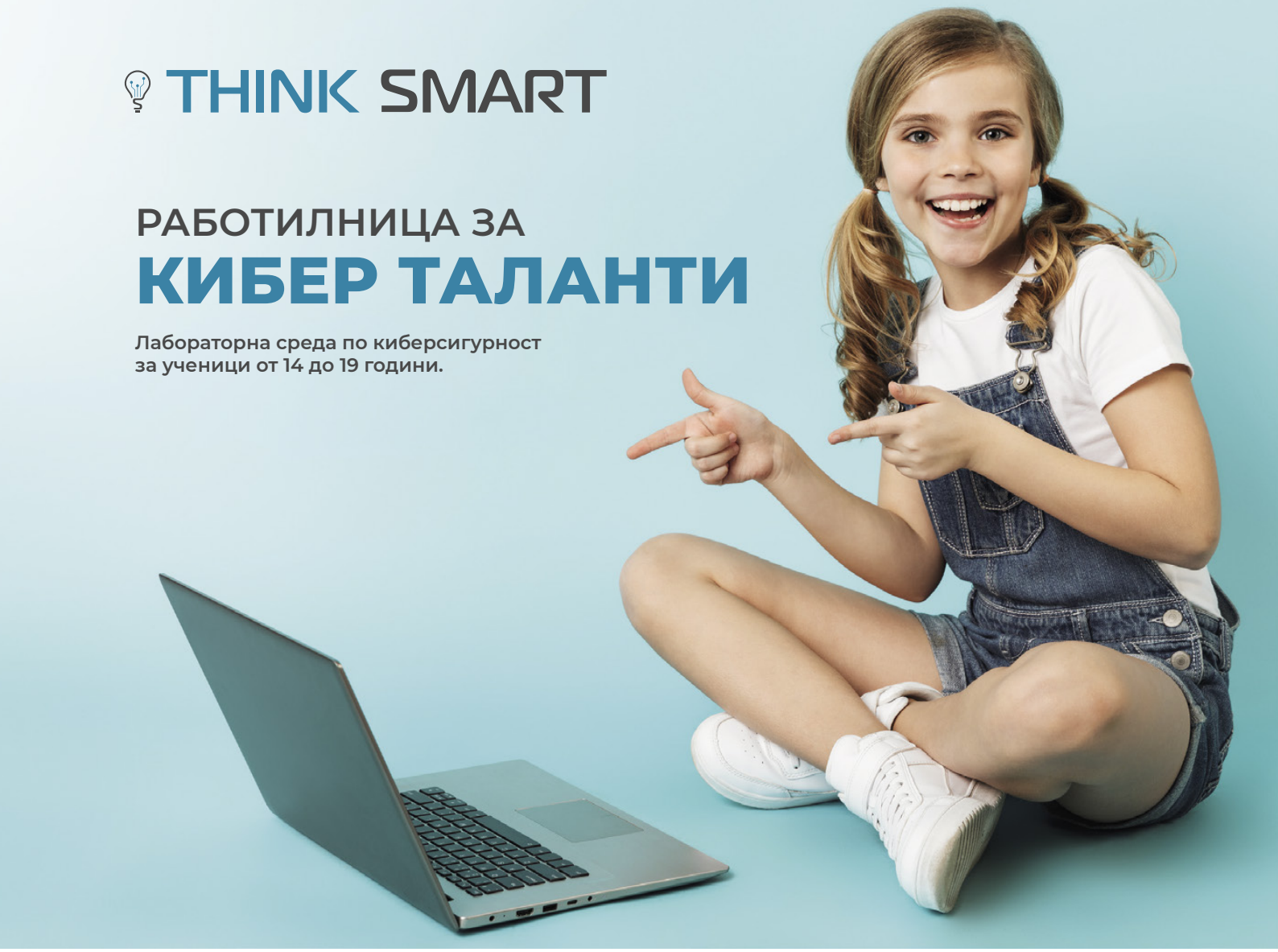
Първата стъпка е в избора на правилния човек вътре в компанията, който да припознае тази задача като своя цел, и след това е изборът на партньорска компания, с която да се върви по този нелек път на гонитба с технологиите. Да, може би страхът продава, но и дисциплинира. „Превенция“ е модерна дума, но аз не бих я използвал толкова често, по-скоро бих казал, че трябва да сме подготвени и да не спираме да се развиваме.

THINK SMART

РАБОТИЛНИЦА ЗА

КИБЕР ТАЛАНТИ

**Лабораторна среда по киберсигурност
за ученици от 14 до 19 години.**



ИСКАШ ДА РАЗВИЕШ СВОИТЕ КИБЕР УМЕНИЯ?

Запиши се при специалистите от THINK SMART.
Докосни се до света на технологиите и черпи знания от най-добрите.
Лабораторията е достъпна всеки делничен ден от 09:00 до 18:00 ч
в офиса на THINK SMART на адрес: ж.к. Младост 1А, ул. Анна Ахматова 9, ет. 5

ЗА ПОВЕЧЕ ИНФОРМАЦИЯ:

0700 100 17

ЗАПИШИ СЕ БЕЗПЛАТНО НА:**

OFFICE@THINKSMART.BG

*Само за ученици на територията на гр. София.
**Допускат се ученици само с предварително записване.

www.THINKSMART.bg

МОГАТ ЛИ РЕГУЛАЦИИТЕ ДА ПОДОБРЯТ КИБЕРСИГУРНОСТТА?

Мария Динкова

Засилената дигитализация, която наблюдаваме във всички сектори от началото на пандемията, доведе със себе си и значителен ръст на кибератаките. На практика за първите шест месеца на 2022 г. седмичните кибернападения са се увеличили с 32% на годишна база, а на всеки 39 секунди се случва един пробив. Освен това в основата на повечето кибератаки присъства фишинг елемент (39%) или са следствие от уязвимост в системите (33%).

В резултат на всички тези онлайн опасности пък общите щети, понесени от бизнеса, тази година достигат 6 трлн. долара.

С подобна статистика гарантирането на киберсигурността се очертава като един от основните въпроси и предизвикателства в съвременния свят. Все по-големите мащаби и въздействие на този вид инциденти излизат извън границите на отделните компании, индустрии и дори държави. А когато последствията не само вредят на фирмения имидж, а заплашват националната сигурност, на преден план неминуемо излиза темата за регулациите и необходимостта от въвеждане на стандарти, които да гарантират една достатъчно висока защита.

Какво е нивото обаче на законовите изисквания и тяхното изпълнение може ли наистина да ни донесе сигурност? Всъщност през последните години основно се коментираха регулациите, свързани с неприкосновеността на данните, но те засягат една много малка част от рисковете, с които се сблъскват компаниите. Миналогодишната атака срещу Colonial Pipeline ясно показа, че е задължително да се предприемат мерки за защитата на цялостната ИТ инфраструктура.

ЗАКОНОВИТЕ ИЗИСКВАНИЯ

„Когато говорим за данни и за киберсигурност, винаги трябва да подхождаме с ясното съзнание, че неприкосновеността на данните и личния живот е крайъгълният камък, фундаменталното човешко право, около което всъщност възниква и се развива киберсигурността като

отделна сфера на регулация. Киберсигурността е функция на правото за неприкосновеност и е основа за защита на това основно право, поради което темите вървят ръка за ръка“, подчертава Никола Стойчев, съдружник в „Димитров, Петров и Ко.“.

Никола Стойчев,
съдружник в "Димитров, Петров и Ко."

Към момента у нас ключово място намират съществуващите актове в областта на защитата на данните (напр. GDPR и ЗЗЛД), но те далеч не са единствените. По думите на експерта съществуват редица регулации, налагащи различни организационни, технологични и технически мерки защита на инфраструктурата. А именно става дума за Закона за киберсигурността (ЗК), Закона за електронното управление, Закона за електронните съобщения, както и няколко наредби за минималните изисквания за мрежова и информационна сигурност и други. В допълнение множество задължения за защита на инфраструктура имат и тесен кръг лица в определени сектори, които управляват критична инфраструктура и обекти, вкл. т. нар. европейска критична инфраструктура.

Стъпвайки на тази основа, можем да обобщим кои са и основните изисквания, на които компаниите в частния и публичния сектор трябва да отговорят:

ОСНОВНИТЕ ИЗИСКВАНИЯ, НА КОИТО КОМПАНИИТЕ В ЧАСТНИЯ И ПУБЛИЧНИЯ СЕКТОР ТРЯБВА ДА ОТГОВОРЯТ, СА:

1. Извършване на анализ и оценка на риска за мрежовата и информационната сигурност.
2. Инфраструктурата да се поддържа по такъв начин, който гарантира, че системите, изпълняващи различни функции, са разделени и изолирани помежду си физически и/или логически.
3. Използване на криптографски механизми, защита на профили с административни права, поддържане на актуален софтуер и фърмуер, достъп да се дава на принципа на строга необходимост и т.н.
4. Наличие на политики относно използването на лични технически средства, записващи устройства, USB и т.н.

Shutterstock

Експертът подчертава, че с прилагането на тези и други мерки всяка компания в голяма степен ще бъде в съответствие с правилата за прилагане на технически и организационни мерки по GDPR. „Разбира се, конкретните мерки винаги ще зависят от естеството на дейността на компанията, възможностите (финансови, технологични и др.), оценката на риска при обработването на данни и други фактори“, изтъква Стойчев. Той припомня, че

вече е одобрена и европейска схема за сертифициране на компании за съответствие с GDPR.

В допълнение трябва да се отбележи, че Законът за киберсигурност предвижда и спазване на редица стандарти за сектора. С други думи, различните мерки за сигурност следва да се прилагат съобразно определени международни стандарти (напр. БДС EN ISO/IEC 27000, 27001 и 27002, БДС ISO 31000, ISO/IEC 11770-1ETSI TS 102 165-1 и много други), съветите на производители и доставчици на софтуер и хардуер, както и с добрите практики, препоръчани от водещи в областта на сигурността организации.

Не на последно място, наскоро Комисията за регулиране на съобщенията също прие Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност. Те засягат не само телеком операторите, а частично и трети лица като доставчици на оборудване и услуги. Последните ще трябва да спазват различни изисквания при сключване на договори, включително адекватни мерки за защита на данни, изисквания за сигурност и достъп на представители и други.

СТИГА ЛИ ТОВА?

Достатъчни ли са обаче тези регулации, за да бъде бизнесът наистина защитен, да се предпази от злонамерените актьори и да предотврати сериозни финансови, имиджови и оперативни щети? Вероятно отговорът се крие във факта, че тепърва предстоят да се въвеж-

дат допълнителни изисквания на национално и европейско ниво през следващите 1 до 3 години. Ключово място в тази връзка заема втората Директива за мрежова и информационна сигурност (NIS 2).

„Нови правила с по-широк обхват на действие ще бъдат въведени с транспонирането на втората Директива за мрежова и информационна сигурност (NIS 2). Тя ще засяга по-голям кръг от лица от частния сектор в сравнение с кръга по Закона за киберсигурността - като ще се разшири до всички средни и големи компании в сектори енергетика, транспорт, банково дело, здравеопазване, цифрова инфраструктура (напр. доставчици на DNS услуги, регистри на имената на домейни от първо ниво, доставчици на облачни услуги, центрове за данни), публична администрация, различни производители и други. В някои сектори като този на телекомуникациите пък задълженията ще обхванат и малките, и микропредприятията“, обяснява Стойчев.

Предвижда се NIS 2 да бъде приета до края на годината или най-късно в началото на 2023 г., след което България ще има 21 месеца да я въведе, като новите изисквания ще бъдат обхванати с изменения в Закона за киберсигурността. Санкциите, които се предвиждат за нарушения, са сходни на тези в GDPR - до 10 млн. евро или до 2% от общия световен годишен оборот на предприятието, която от сумите е по-голяма.

Отделно предстои приемане на секторен Регламент относно оперативната устойчивост на цифровите технологии във финансовия сектор, както и Директива относно устойчивостта на критичните субекти и други.

Междувременно пък Агенцията на Европейския съюз за киберсигурност работи по първата европейска схема за сертифициране на киберсигурността. По нея ще бъдат оценявани продукти, услуги и процеси на информационните и комуникационните технологии за съответствие спрямо специфичните изисквания за защита.

РЕГУЛАЦИИТЕ КАТО РИСК

Едва ли можем да поставим под съмнение факта, че въвеждането на повече регулации в сферата на киберсигурността ще донесе редица ползи както на обществото като цяло, така и на всеки отделен бизнес. „Наличието на хармонизирани изисквания на ниво ЕС ще осигури предвидимост и сигурност за гражданите, за ползваните обществени услуги, ще подобри общата среда и готовност за реакция в случай на заплахи за киберсигурността“, посочва Стойчев.

В същото време компаниите ще могат да се радват на по-голяма устойчивост, последвана от успешно развитие и доволни партньори и клиенти. Според експерта мерките позволяват уязвимостта да се сведе до наистина сериозни атаки, тъй като по-голямата част от кибернападенията са слаби по интензитет и не особено сложни. Съответно лесно могат да бъдат предотвратени със сравнително базови защити и познаване на опасностите.

Уловката обаче се крие в това, че изискванията трябва да са ясни и сравнително лесни за изпълнение. А балансът понякога е труден за постигане, особено когато из-

изква властите да са кооперативни и по-често да дават възможност за отстраняване на по-дребни нарушения, преди да пристъпят към санкции; както и при необходимост да предоставят своевременно тълкуване на спорни въпроси.

Освен това регулациите сами по себе си създават допълнителна тежест за бизнеса, тъй като налагат да се инвестират значителни финансови и човешки ресурси за подготовка и дългосрочно спазване на изискванията. Например те внасят нови административни задължения за изготвяне на вътрешни документи като политики, процедури, оценки и т.н.

КРАЧКИ В ПРАВИЛНАТА ПОСОКА

Независимо от предизвикателствата, съпътстващи гарантирането на съответствие, не трябва да забравяме причината за въвеждането на мерките - а именно опасността и сериозните вреди, които кибератаките нанасят.

На фона на предстоящите нови регулации определено всяка компания трябва да обърне поглед към вътрешните си процеси, за да идентифицира пропуски в дейността си, които могат да я изложат на риска. Стойчев препоръчва да се започне от проверка на спазването на изискванията на GDPR за осигуряване на технически и организационни мерки за защита (в това число изготвяне на вътрешна документация).

„Компаниите, които не са направили анализи или имат съмнения, е препоръчително да проверят дали не попа-

дат в обхвата на ЗК или други приложими актове. Ако се окаже, че това е така, съответно трябва да пристъпят към прилагане на тези изисквания. За компаниите пък, които не са в обхвата на ЗК, е препоръчително да започнат полека да внедряват различни мерки за защита“, съветва експертът. По този начин те не само ще бъдат подготвени срещу кибер- и физически атаки, но също така ще бъдат в крак с влизането в сила на NIS 2 и редица други актове, касаещи специфични сектори.

Това важи в пълна степен за организациите, които попадат в обхвата на новите изисквания, както за доставчици на различни продукти/услуги на задължени лица по NIS 2 и другите специфични секторни актове. „Последните ще трябва да се подготвят за проверки и искания на информация от лицата в обхвата на NIS 2 и други актове (напр. телеком оператори) и ще трябва да могат да гарантират и доказват, че са налице ефективни, документирани процеси за управление на рисковете за сигурността, свързани с предлаганите от тях продукти/услуги“, отбелязва Стойчев.

Все пак големият въпрос остава - стигат ли тези регулации и допринасят ли за повишаване на киберсигурността? Наличието на законови изисквания е важна стъпка в правилната посока, но тя рядко е достатъчна. Мерките трябва да се спазват, а тези, които не полагат достатъчно усилия, да бъдат санкционирани. В противен случай ще имаме добре разписани регулации на хартия, които обаче не се отразяват в реалния и виртуалния свят.

„Индустриална киберсигурност“
е анализ на Digitalk.

Digitalk е платформа за технологии и бизнес. Нейната функция е да информира и свързва хората, които работят в сферата на информационните технологии или искат да трансформират бизнеса си чрез тях.

Издатели:
Иво Прокопиев
Теодор Захов

Изпълнителен директор:
Галя Прокопиева

Главен редактор:
Деница Дженева

Отговорен редактор:
Александър Главчев

Редактори:
Владимир Владков
Иван Гайдаров
Майя Бойчева-Манолчева
Мария Динкова

Дизайн и предпечат:
Марияна Попова

Коректори:
Диляна Енчева
Милена Братованова

Редакция:
1000 София, ул. „Иван Вазов“ 20
тел. 02/4615 410
editors@digitalk.bg

Реклама:
тел. 02/ 4615 444
reklama@economedia.bg

Абонамент:
тел. 02/ 4615 349
abonament@economedia.bg